USER GUIDE

Simultaneous Dual-N Band Wireless Router

Model: WRT610N

About This Guide

Icon Descriptions

While reading through the User Guide you may see various icons that call attention to specific items. Below is a description of these icons:

NOTE: This check mark indicates that there is a note of interest and is something that you should pay special attention to while using the product.

WARNING: This exclamation point indicates that there is a caution or warning and it is something that could damage your property or product.

WEB: This globe icon indicates a noteworthy website address or e-mail address.

Online Resources

Website addresses in this document are listed without **http://** in front of the address because most current web browsers do not require it. If you use an older web browser, you may have to add **http://** in front of the web address.

Resource	Website
Linksys	www.linksys.com
Linksys International	www.linksys.com/international
Glossary	www.linksys.com/glossary
Network Security	www.linksys.com/security

Copyright and Trademarks

Linksys is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries. Copyright © 2008 Cisco Systems, Inc. All rights reserved. Other brands and product names are trademarks or registered trademarks of their respective holders.

Chapter 1: Product Overview 3

Front Panel . . . 3
Back Panel . . . 3

Chapter 2: Wireless Security Checklist 5

General Network Security Guidelines . . . 5
Additional Security Tips . . . 5

Chapter 3: Advanced Configuration 6

Setup > Basic Setup . . . 6
Setup > MAC Address Clone . . . 11
Setup > Advanced Routing . . . 11
Wireless > Basic Wireless Settings . . . 12
Wireless > Wireless MAC Filter . . . 16
Wireless > Advanced Wireless Settings . . . 17
Security > Firewall . . . 18
Security > VPN Passthrough . . . 18
Storage > Disk . . . 19
Storage > Media Server . . . 20
Storage > FTP Server . . . 21
Storage > Administration . . . 22
Access Restrictions > Internet Access . . . 23
Applications and Gaming > Port Range Forwarding . . . 25
Applications & Gaming > Port Triggering . . . 25
Applications and Gaming > DMZ . . . 26
Applications and Gaming > QoS . . . 26
Administration > Management . . . 29
Administration > Log . . . 29
Administration > Diagnostics . . . 30
Administration > Factory Defaults . . . 30
Administration > Firmware Upgrade . . . 30
Status > Router . . . 31
Status > Local Network . . . 31
Status > Wireless Network . . . 32

Appendix A: Troubleshooting 33

Appendix B: How to Install and Access USB Storage 34

Overview . . . 34
How to Install the USB Storage . . . 34
How to Access the USB Storage . . . 34
Advanced Configuration (Advanced Users Only) . . . 38

Appendix C: Specifications 41

Appendix D: Warranty Information 42

Limited Warranty 42
Exclusions and Limitations. 42
Obtaining Warranty Service 42
Technical Support 43

Appendix E: Regulatory Information 44

FCC Statement 44
FCC Radiation Exposure Statement 44
Safety Notices. 44
Wireless Disclaimer 44
Industry Canada Statement 44
Restrictions in the 5 GHz Band 45
Avis d’Industrie Canada. 45
Avis de non-responsabilité concernant les appareils sans fil 45
User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE) 46

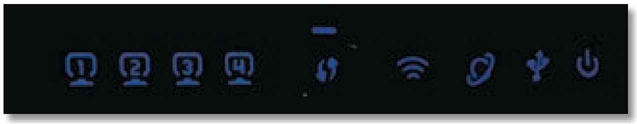
Appendix F: Software License Agreement 50

Software in Linksys Products 50
Software Licenses 50

Chapter 1:
Product Overview

Thank you for choosing the Dual-Band Wireless-N Gigabit Router with Storage Link. The Router lets you access the Internet via a wireless connection or through one of its four switched ports. With the built-in storage link, you can easily add gigabytes of storage space onto your network using USB 2.0 hard drives, or plug in a USB flash disk to access your portable data files. The built-in media server streams music, video and photos from the attached storage device to any UPnP-compatible media adapter. Configuring the Router is easy using the provided browser-based utility.

Front Panel



1, 2, 3, 4 (Green/Blue) These numbered LEDs, corresponding with the numbered ports on the Router's back panel, serve two purposes. If the LED is continuously lit, the Router is successfully connected to a device through that port. A flashing LED indicates network activity over that port. The LED lights up Green when it is connected to gigabit port and Blue when it is connected to a 10/100 port.

Wi-Fi Protected Setup Button If you have client devices, such as wireless adapters, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup to automatically configure wireless security for your wireless network(s).

To use Wi-Fi Protected Setup, run the Linksys Easy Link Advisor (LELA) , or refer to the "Wireless > Basic Wireless Settings" section of "Chapter 3: Advanced Configuration".

Wi-Fi Protected Setup (WPS) LED (Blue/ Amber) The LED flashes blue for two minutes during the WPS process and lights up blue when the WPS process is successful.

The LED lights up amber if there is an error during the Wi-Fi Protected Setup process. Make sure the client device supports Wi-Fi Protected Setup. Wait until the LED is off, and then try again.

The LED flashes when a Wi-Fi Protected Setup session is active. The Router supports one session at a time. Wait until the LED is solidly lit, or off before starting the next Wi-Fi Protected Setup session.

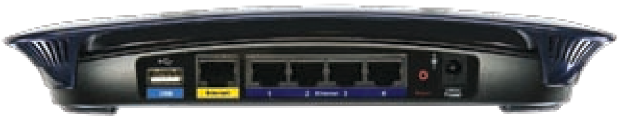
Wireless (Blue) The Wireless LED lights up when the wireless feature is enabled. If the LED is flashing, the Router is actively sending or receiving data over the network.

Internet (Green/Blue) The Internet LED lights up when there is a connection made through the Internet port. A flashing LED indicates network activity over the Internet port. The LED lights up Green when it is connected to gigabit port and Blue when it is connected to a 10/100 port.

USB (Blue) The USB LED lights up when a USB device is attached. If the LED is flashing, the data is being sent or received through this device.

Power (Blue) The Power LED lights up and will stay on while the Router is powered on. When the Router goes through its self-diagnostic mode during every boot-up, this LED will flash. When the diagnostic is complete, the LED will be solidly lit.

Back Panel



USB Port For use with an external hard drive.

Internet The Internet port is where you will connect your cable or DSL Internet connection.

1, 2, 3, 4 These Ethernet ports (1, 2, 3, 4) connect the Router to PCs on your wired network and other Ethernet network devices.

Reset There are two ways to reset the Router's factory defaults. Either press and hold the Reset Button for approximately five seconds, or restore the defaults from Administration > Factory Defaults in the Router's web-based utility.

Power The Power port is where you will connect the power adapter.

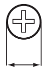
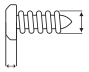
Horizontal Placement

The Router has four rubber feet on its bottom panel. Place the Router on a level surface near an electrical outlet.

Wall-Mounting Placement

The Router has two wall-mount slots on its bottom panel. The distance between the slots is 175.56 mm (6.91 inches).

Two screws are needed to mount the Router.

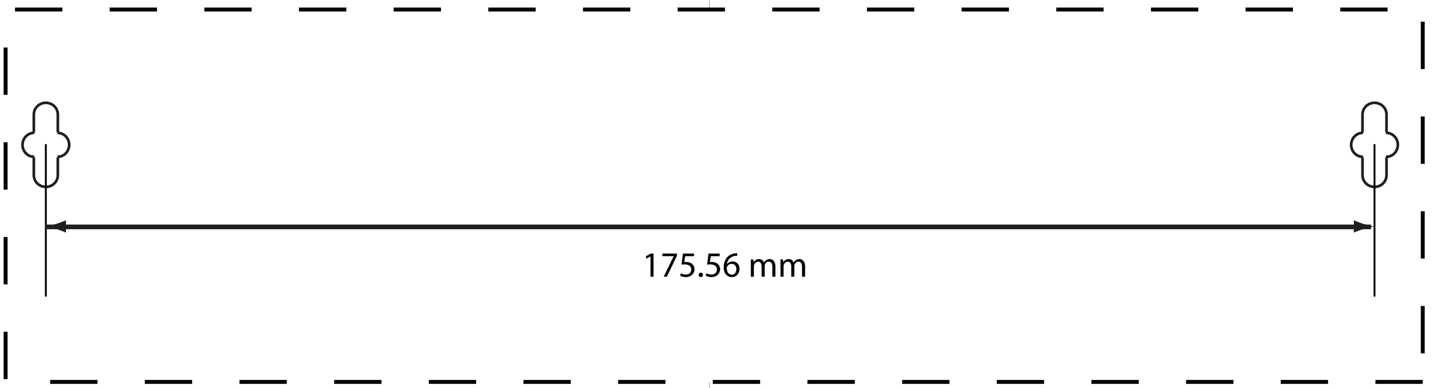
Suggested Mounting Hardware		
 4-5 mm	 1-1.5 mm	2.5-3.0 mm

†Note: Mounting hardware illustrations are not true to scale.

NOTE: Linksys is not responsible for damages incurred by unsecure wall-mounting hardware.

Follow these instructions:

1. Determine where you want to mount the Router. Make sure that the wall you use is smooth, flat, dry, and sturdy. Also make sure the location is within reach of an electrical outlet.
2. Drill two holes into the wall. Make sure the holes are 175.56 mm (6.91 inches) apart.
3. Insert a screw into each hole and leave 3 mm (0.12 inches) of its head exposed.
4. Maneuver the Router so the wall-mount slots line up with the two screws.
5. Place the wall-mount slots over the screws and slide the Router down until the screws fit snugly into the wall-mount slots.



Chapter 2: Wireless Security Checklist

Wireless networks are convenient and easy to install, so homes with high-speed Internet access are adopting them at a rapid pace. Because wireless networking operates by sending information over radio waves, it can be more vulnerable to intruders than a traditional wired network. Like signals from your cellular or cordless phones, signals from your wireless network can also be intercepted. Since you cannot physically prevent someone from connecting to your wireless network, you need to take some additional steps to keep your network secure.

1. Change the default wireless network name or SSID

Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network, and can be up to 32 characters in length. Linksys wireless products use **linksys** as the default wireless network name. You should change the wireless network name to something unique to distinguish your wireless network from other wireless networks that may exist around you, but do not use personal information (such as your Social Security number) because this information may be available for anyone to see when browsing for wireless networks.

2. Change the default password

For wireless products such as access points and routers, you will be asked for a password when you want to change their settings. These devices have a default password set by the factory. The Linksys default password is **admin**. Hackers know these defaults and may try to use them to access your wireless device and change your network settings. To thwart any unauthorized changes, customize the device's password so it will be hard to guess.

3. Enable MAC address filtering

Linksys routers give you the ability to enable Media Access Control (MAC) address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device. With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify the MAC address of each computer in your home so that only those computers can access your wireless network.

4. Enable encryption

Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalency Privacy (WEP) offer different levels of security for wireless communication.

A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment.

WEP is an older encryption standard and may be the only option available on some older devices that do not support WPA.

General Network Security Guidelines

Wireless network security is useless if the underlying network is not secure.

- Password protect all computers on the network and individually password protect sensitive files.
- Change passwords on a regular basis.
- Install anti-virus software and personal firewall software.
- Disable file sharing (peer-to-peer). Some applications may open file sharing without your consent and/or knowledge.

Additional Security Tips

- Keep wireless routers, access points, or gateways away from exterior walls and windows.
- Turn wireless routers, access points, or gateways off when they are not being used (at night, during vacations).
- Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary.

WEB: For more information on wireless security, visit **www.linksys.com/security**

Chapter 3: Advanced Configuration

After setting up the Router with the Setup Wizard (located on the CD-ROM), the Router will be ready for use. If you'd like to change its advanced settings, use the Router's web-based utility. This chapter describes each web page of the utility and each page's key functions. You can access the utility via a web browser on a computer connected to the Router.

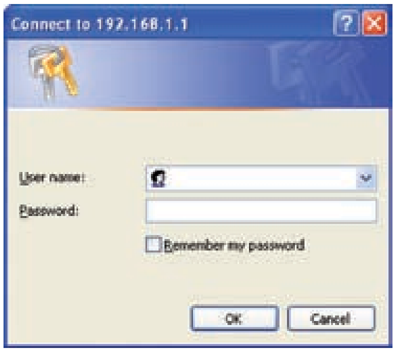
The web-based utility has these main tabs: Setup, Wireless, Security, Storage, Access Restrictions, Applications & Gaming, Administration, and Status. Additional tabs will be available after you click one of the main tabs.

NOTE: When you first install the Router, you should use the Setup Wizard on the Setup CD-ROM. If you want to configure advanced settings, use this chapter to learn about the web-based utility.

How to Access the Web-Based Utility

To access the web-based utility, launch the web browser on your computer, and enter the Router's default IP address, **192.168.1.1** or **http://wrt160n.com** in the *Address* field. Then, press **Enter**.

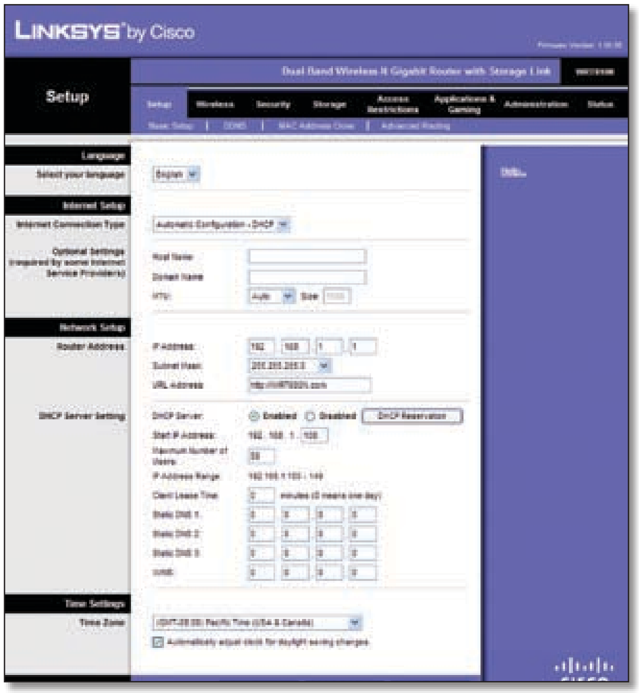
A password request screen will appear. (Non-Windows XP users will see a similar screen.) Leave the *User name* field blank. The first time you open the web-based utility, use the default password **admin**. (You can set a new password on the Administration > Management screen.) Click **OK** to continue.


Connect to 192.168.1.1
User name:
Password:
☐ Remember my password
OK
Cancel

Password Screen

Setup > Basic Setup

The first screen that appears is the *Basic Setup* screen. This allows you to change the Router's general settings.


LINKSYS by Cisco
Setup
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Language
Internet Setup
Network Setup
Time Settings

Setup > Basic Setup

Language

Language To use a different language, select one from the drop-down menu. The language of the web-based utility will change five seconds after you select another language.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Internet Setup

The Internet Setup section configures the Router to your Internet connection. Most of this information can be obtained through your Internet Service Provider (ISP).

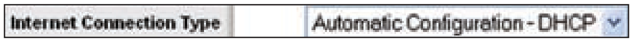
Internet Connection Type

Select the type of Internet connection your ISP provides from the drop-down menu. The available types are:

- Automatic Configuration - DHCP
- Static IP
- PPPoE
- PPTP
- L2TP
- Telstra Cable

Automatic Configuration - DHCP

By default, the Router's Internet Connection Type is set to **Automatic Configuration - DHCP**, which should be kept only if your ISP supports DHCP or you are connecting through a dynamic IP address. (This option usually applies to cable connections.)

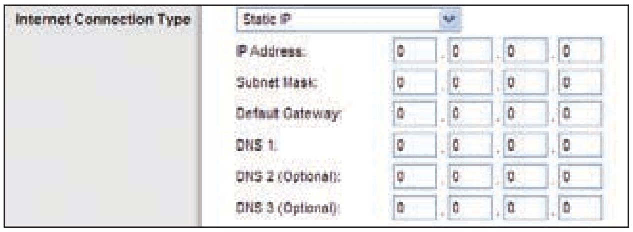


Internet Connection Type: Automatic Configuration - DHCP

Internet Connection Type > Automatic Configuration - DHCP

Static IP

If you are required to use a permanent IP address to connect to the Internet, select **Static IP**.



Internet Connection Type: Static IP
IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Default Gateway: 0 . 0 . 0 . 0
DNS 1: 0 . 0 . 0 . 0
DNS 2 (Optional): 0 . 0 . 0 . 0
DNS 3 (Optional): 0 . 0 . 0 . 0

Internet Connection Type > Static IP

IP Address This is the Router's IP address, when seen from the Internet. Your ISP will provide you with the IP Address you need to enter here.

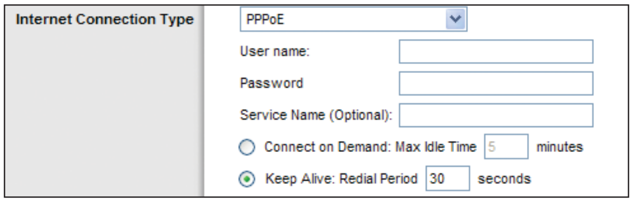
Subnet Mask This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway Your ISP will provide you with the Gateway Address, which is the ISP server's IP address.

DNS Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, you will have to enable **PPPoE**.



Internet Connection Type: PPPoE
User name:
Password
Service Name (Optional):
○ Connect on Demand: Max Idle Time 5 minutes
● Keep Alive: Redial Period 30 seconds

Internet Connection Type > PPPoE

User Name and Password Enter the User Name and Password provided by your ISP.

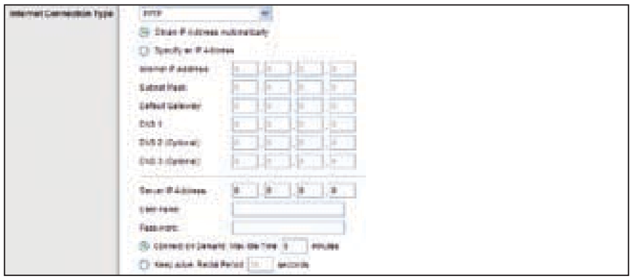
Service Name (optional) If provided by your ISP, enter the Service Name.

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes.

Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select **Keep Alive**. In the *Redial Period* field, you specify how often you want the Router to check the Internet connection. The default Redial Period is **30** seconds.

PPTP

Point-to-Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only.



Internet Connection Type > PPTP

If your ISP supports DHCP or you are connecting through a dynamic IP address, then select **Obtain an IP Address Automatically**. If you are required to use a permanent IP address to connect to the Internet, then select **Specify an IP Address**. Then configure the following:

Internet IP Address This is the Router's IP address, as seen from the Internet. Your ISP will provide you with the IP Address you need to specify here.

Subnet Mask This is the Router's Subnet Mask, as seen by users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway Your ISP will provide you with the Gateway Address, which is the ISP server's IP address.

DNS Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

Server IP Address Your ISP will provide you with the Server IP Address.

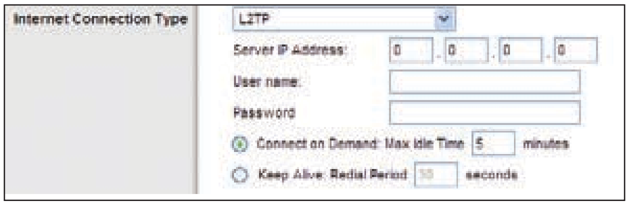
User Name and Password Enter the User Name and Password provided by your ISP.

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes.

Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select **Keep Alive**. In the *Redial Period* field, specify how often you want the Router to check the Internet connection. The default value is **30** seconds.

L2TP

L2TP is a service that applies to connections in Israel only.



Internet Connection Type: L2TP

Server IP Address: 0 . 0 . 0 . 0

User name:

Password

● Connect on Demand: Max Idle Time 5 minutes

○ Keep Alive: Redial Period 30 seconds

Internet Connection Type > L2TP

Server IP Address This is the IP address of the L2TP Server. Your ISP will provide you with the IP Address you need to specify here.

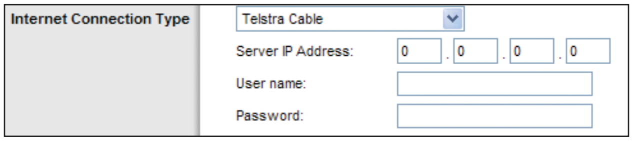
User Name and Password Enter the User Name and Password provided by your ISP.

Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the *Max Idle Time* field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes

Keep Alive: Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select **Keep Alive**. In the *Redial Period* field, you specify how often you want the Router to check the Internet connection. The default Redial Period is **30** seconds.

Telstra Cable

Telstra Cable is a service that applies to connections in Australia only.



Internet Connection Type: Telstra Cable

Server IP Address: 0 . 0 . 0 . 0

User name:

Password:

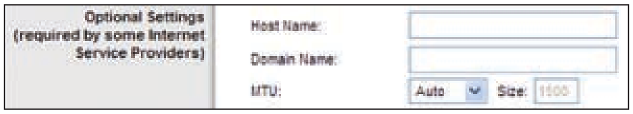
Internet Connection Type > Telstra Cable

Server IP Address This is the IP address of the Telstra Cable. Your ISP will provide you with the IP Address you need to specify here.

User Name and Password Enter the User Name and Password provided by your ISP.

Optional Settings

Some of these settings may be required by your ISP. Verify with your ISP before making any changes.



Optional Settings (required by some Internet Service Providers)

Host Name:

Domain Name:

MTU: Auto Size: 1500

Optional Settings

Host Name/Domain Name These fields allow you to supply a host and domain name for the Router. Some ISPs, usually cable ISPs, require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

MTU MTU is the Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. Select Manual if you want to manually enter the largest packet size that is transmitted. To have the Router select the best MTU for your Internet connection, keep the default setting, **Auto**.

Size When Manual is selected in the *MTU* field, this option is enabled. Leave this value in the 1200 to 1500 range. The default size depends on the Internet Connection Type:

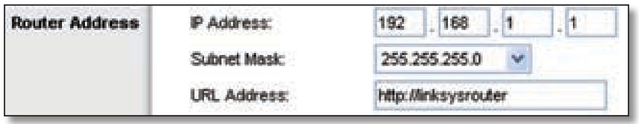
- DHCP, Static IP, or Telstra: **1500**
- PPPoE: **1492**
- PPTP or L2TP: **1460**

Network Setup

The Network Setup section changes the settings on the network connected to the Router's Ethernet ports. Wireless Setup is performed through the Wireless tab.

Router Address

This presents both the Router's IP Address, Subnet Mask, and URL Address as seen by your network. The default Router IP address is **192.168.1.1** and URL address is **http://WRT610N.com**.

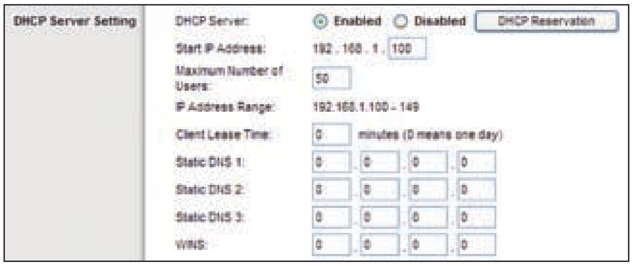


IP Address: 192 . 168 . 1 . 1
Subnet Mask: 255.255.255.0
URL Address: http://linksysrouter

Router IP Address

Network Address Server Settings (DHCP)

The settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the Router's DHCP server option, make sure there is no other DHCP server on your network.



DHCP Server: ● Enabled ○ Disabled
Start IP Address: 192 . 168 . 1 . 100
Maximum Number of Users: 50
IP Address Range: 192.168.1.100 - 149
Client Lease Time: 0 minutes (0 means one day)
Static DNS 1: 0 . 0 . 0 . 0
Static DNS 2: 0 . 0 . 0 . 0
Static DNS 3: 0 . 0 . 0 . 0
WINS: 0 . 0 . 0 . 0

Network Address Server Settings (DHCP)

DHCP Server DHCP is enabled by factory default. If you already have a DHCP server on your network, or you don't want a DHCP server, then select **Disabled** (no other DHCP features will be available).

Starting IP Address Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router's default IP address is **192.168.1.1**, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.253. The default Starting IP Address is **192.168.1.100**.

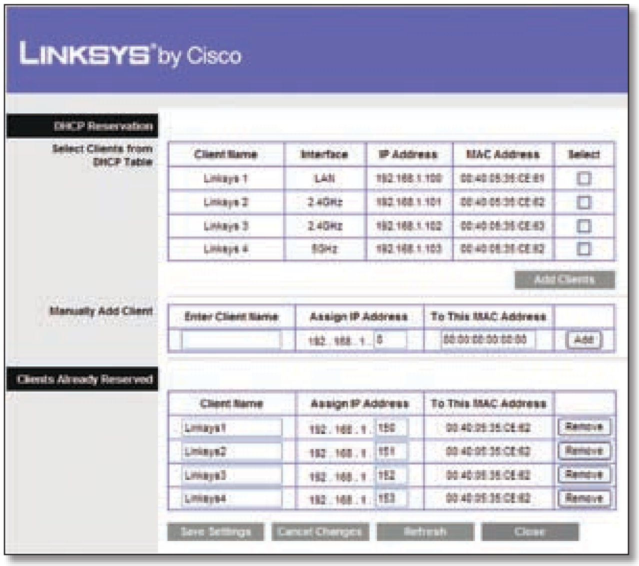
Maximum Number of DHCP Users Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. The default is **50**.

Client Lease Time The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address. After the time is up, the user will be automatically assigned a new dynamic IP address. The default is **0** minutes, which means one day.

Static DNS (1-3) The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, enter that IP Address in one of these fields. You can enter up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers.

WINS The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that server's IP Address here. Otherwise, leave this blank.

DHCP Reservation Click **DHCP Reservation** if you want to assign a fixed local IP address to a MAC address.



Client Name	Interface	IP Address	MAC Address	Select
Linksys 1	LAN	192.168.1.100	00:40:05:35:CE:81	☐
Linksys 2	2.4GHz	192.168.1.101	00:40:05:35:CE:82	☐
Linksys 3	2.4GHz	192.168.1.102	00:40:05:35:CE:83	☐
Linksys 4	5GHz	192.168.1.103	00:40:05:35:CE:82	☐

Enter Client Name	Assign IP Address	To This MAC Address	
	192 . 168 . 1 . 0	00:00:00:00:00:00	Add

Client Name	Assign IP Address	To This MAC Address	
Linksys1	192 . 168 . 1 . 150	00:40:05:35:CE:82	Remove
Linksys2	192 . 168 . 1 . 151	00:40:05:35:CE:82	Remove
Linksys3	192 . 168 . 1 . 152	00:40:05:35:CE:82	Remove
Linksys4	192 . 168 . 1 . 153	00:40:05:35:CE:82	Remove

DHCP Reservation

You will see a list of DHCP clients with the following information: Client Name, Interface, IP Address, and MAC Address. Click the **Select** checkbox to reserve a client's IP address. Then click **Add Clients**.

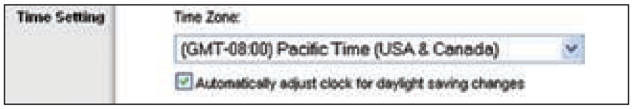
If you want to manually assign an IP address, enter the client's name in the *Enter Client Name* field. Enter the IP address you want it to have in the *Assign IP Address* field. Make sure the IP address is between the starting DHCP server's IP address and maximum number of DHCP users range. Enter its MAC Address in the *To This MAC Address* field. Click **Add**.

A list of DHCP clients and their fixed local IP addresses will be displayed at the bottom of the screen. If you want to remove a client from this list, click **Remove**.

When you finish your changes, click **Save Settings** to save your changes. Click **Cancel Changes** to cancel your changes. To view the most up-to-date information, click **Refresh**. To exit this screen, click **Close**.

Time Setting

Select the time zone in which your network functions from this drop-down menu. (You can even automatically adjust for daylight saving time.)



Time Setting

Time Zone:

(GMT-08:00) Pacific Time (USA & Canada)

☑ Automatically adjust clock for daylight saving changes

Time Setting

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Setup > DDNS

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router.

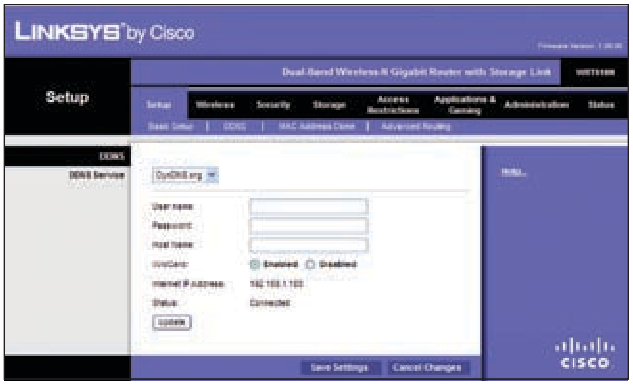
Before you can use this feature, you need to sign up for DDNS service with a DDNS service provider, www.dyndns.org or www.TZO.com. If you do not want to use this feature, keep the default setting, **Disabled**.

DDNS

DDNS Service

If your DDNS service is provided by DynDNS.org, then select **DynDNS.org** from the drop-down menu. If your DDNS service is provided by TZO, then select **TZO.com**. The features available on the *DDNS* screen will vary, depending on which DDNS service provider you use.

DynDNS.org


LINKSYS by Cisco
Setup
Dual-Band Wireless-N Gigabit Router with Storage Link
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
DDNS
DDNS Service
DynDNS.org
User name
Password
Host Name
WildCard
Enabled
Disabled
Internet IP Address
Status
Connected
Update
Help...
Save Settings
Cancel Changes
CISCO

Setup > DDNS > DynDNS

User Name Enter the User Name for your DDNS account.

Password Enter the Password for your DDNS account.

Host Name The is the DDNS URL assigned by the DDNS service.

WildCard Select **Enabled** to enable this feature or **Disabled** to disable it.

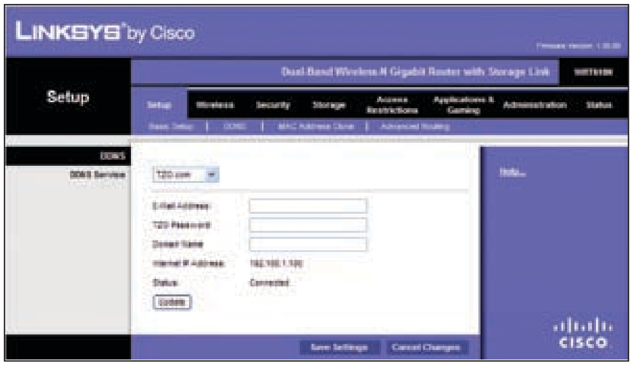
Internet IP Address The Router's Internet IP address is displayed here. Because it is dynamic, it will change.

Status The status of the DDNS service connection is displayed here.

Update To manually trigger an update, click **Update**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

TZO.com


LINKSYS by Cisco
Setup
Dual-Band Wireless-N Gigabit Router with Storage Link
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
DDNS
DDNS Service
TZO.com
E-Mail Address
TZO Password
Domain Name
Internet IP Address
Status
Connected
Update
Help...
Save Settings
Cancel Changes
CISCO

Setup > DDNS > TZO

E-mail Address, TZO Password, and Domain Name Enter the settings of the account you set up with TZO.

Internet IP Address The Router's Internet IP address is displayed here. Because it is dynamic, it will change.

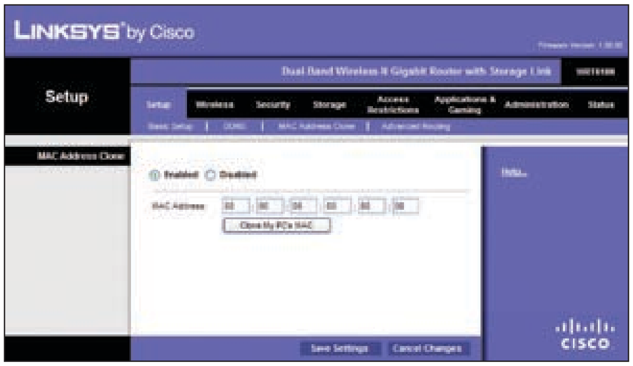
Status The status of the DDNS service connection is displayed here.

Update To manually trigger an update, click **Update**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Setup > MAC Address Clone

Every computere hardware device, including the network adapter of your computer has a unique code called a MAC address. Some Internet Service Providers (ISPs) require you to register this address with them in order to access the Internet. If you do not wish to re-register the MAC address with your ISP, you may assign the MAC address you have currently registered with your ISP to the Router with the MAC Address Clone feature.


LINKSYS by Cisco
Dual-Band Wireless-N Gigabit Router with Storage Link
Setup
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Basic Setup
DDNS
MAC Address Clone
Advanced Routing
MAC Address Clone
Enabled
Disabled
MAC Address
Clone My PC's MAC
Help...
Save Settings
Cancel Changes
CISCO

Setup > MAC Address Clone

MAC Address Clone

Enabled/Disabled To enable MAC Address cloning, select **Enabled**.

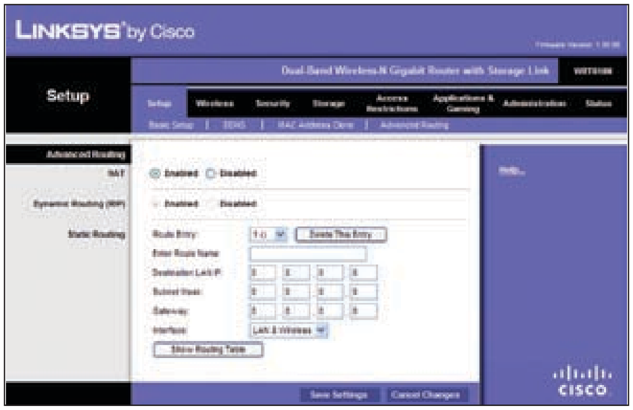
User Defined Entry Enter the MAC Address registered with your ISP here.

Clone Your PC's MAC Clicking this button will clone the MAC address of the computer you are using.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Setup > Advanced Routing

This screen is used to set up the Router's advanced functions. Operating Mode allows you to select the type(s) of advanced functions you use. Dynamic Routing automatically adjusts how packets travel on your network. Static Routing sets up a fixed route to another network destination.


LINKSYS by Cisco
Dual-Band Wireless-N Gigabit Router with Storage Link
Setup
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Basic Setup
DDNS
MAC Address Clone
Advanced Routing
Advanced Routing
NAT
Enabled
Disabled
Dynamic Routing (RIP)
Enabled
Disabled
Static Routing
Route Entry
Delete This Entry
Enter Route Name
Destination LAN IP
Subnet Mask
Gateway
Interface
LAN & Wireless
Show Routing Table
Help...
Save Settings
Cancel Changes
CISCO

Setup > Advanced Routing

Advanced Routing

NAT If this Router is hosting your network's connection to the Internet, select **Enabled**. When NAT is disabled, **Dynamic Routing (RIP)** will be available as an option.

Dynamic Routing (RIP) This feature enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with the other router(s). The Router determines the network packets' route based on the fewest number of hops between the source and the destination. This feature is **Disabled** by default.

Static Routing

Select Route Entry number To set up a static route between the Router and another network, select a number from the drop-down list. (A static route is a pre-determined pathway that network information must travel to reach a specific host or network.) Enter the information described below to set up a new static route. (Click **Delete This Entry** to delete a static route.)

Enter Route Name Enter a name for the Route here, using a maximum of 25 alphanumeric characters.

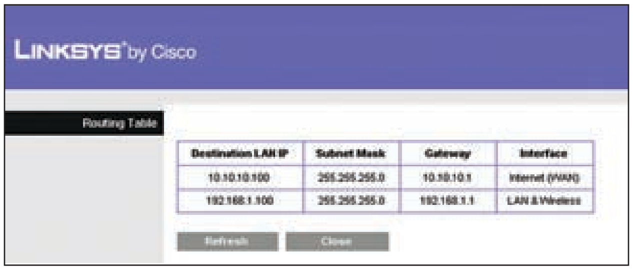
Destination LAN IP The Destination LAN IP is the address of the remote network or host to which you want to assign a static route.

Subnet Mask The Subnet Mask determines which portion of a Destination LAN IP address is the network portion, and which portion is the host portion.

Gateway This is the IP address of the gateway device that allows for contact between the Router and the remote network or host.

Interface This interface tells you whether the Destination IP Address is on the **LAN & Wireless** (Ethernet and wireless networks) or the **WAN (Internet)**.

Click **Show Routing Table** to view the Static Routes you have already set up.


LINKSYS by Cisco
Routing Table
Refresh
Close

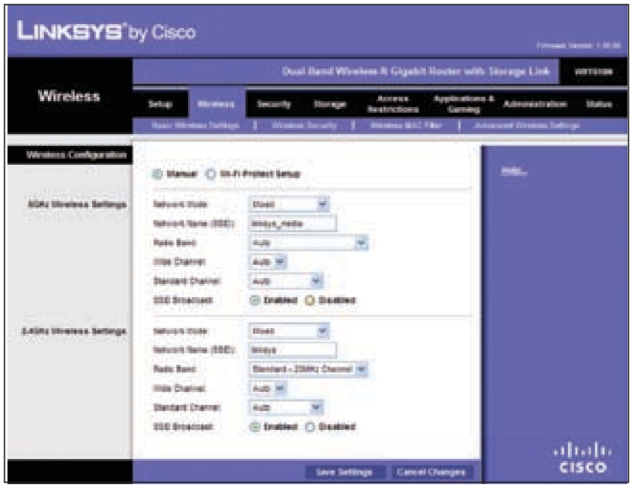
Destination LAN IP	Subnet Mask	Gateway	Interface
10.10.10.100	255.255.255.0	10.10.10.1	Internet (WAN)
192.168.1.100	255.255.255.0	192.168.1.1	LAN & Wireless

Routing Table

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wireless > Basic Wireless Settings

The basic settings for wireless networking are set on this screen.


LINKSYS by Cisco
Dual-Band Wireless-N Gigabit Router with Storage Link
Wireless
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings
Wireless Security
Wireless MAC Filter
Advanced Wireless Settings
Wireless Configuration
Manual
Wi-Fi Protect Setup
5GHz Wireless Settings
2.4GHz Wireless Settings
Help...
Save Settings
Cancel Changes
CISCO

Wireless > Basic Wireless Settings

Wireless Configuration

Wireless Configuration Keep the default selection, **Wi-Fi Protected Setup** to configure your network using Wi-Fi Protected Setup. Select **Manual** to set up your wireless network your wireless network manually.

Manual

If you set the *Wireless Configuration* to **Manual**, the *Basic Wireless Settings* screen displays the following fields.

Network Mode (5 GHz) From this drop-down menu, you can select the wireless standards running on your network. If you have both Wireless-A and Wireless-N (5GHz) devices in your network, keep the default setting, **Mixed**. If you have only Wireless-A devices, select **Wireless-A Only**. If you have only Wireless-N (5GHz) devices, select **Wireless-N Only.** If you do not have any Wireless-A and Wireless-N (5GHz) devices in your network, select **Disabled**.

Network Mode (2.4 GHz) From this drop-down menu, you can select the wireless standards running on your network. If you have both Wireless-B, Wireless-G and Wireless-N (2.4GHz) devices in your network, keep the default setting, **Mixed**. If you have only Wireless-B devices, select **Wireless-B Only**. If you have only Wireless-G devices, select **Wireless-G Only**. If you have only Wireless-N (2.4GHz) devices, select **Wireless-N Only**. If you do not have any Wireless-B, Wireless-G and Wireless-N (2.4GHz) devices in your network, select **Disabled**.

Wireless Network Name (SSID) The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 keyboard characters. Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID to a unique name.

Radio Band (5 GHz) For best performance in a network using Wireless-A and Wireless-N (5GHz) devices, keep the default, **Auto**.

Radio Band (2.4 GHz) For best performance in a network using Wireless-B, Wireless-G and Wireless-N (2.4GHz) devices, select **Auto**. The default is **Standard - 20MHz Channel**.

Wide Channel (5 GHz) If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N (5GHz) channel. If you are not sure which channel to select, keep the default, **Auto (DFS)**.

Wide Channel (2.4 GHz) If you selected Wide - 40MHz Channel for the Radio Band setting, then this setting will be available for your primary Wireless-N (2.4GHz) channel. If you are not sure which channel to select, keep the default, **Auto**.

Standard Channel (5 GHz) Select the channel for Wireless-A and Wireless-N (5GHz) networking. If you selected Wide – 40MHz Channel for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N (5GHz). If you are not sure which channel to select, keep the default, **Auto (DFS)**.

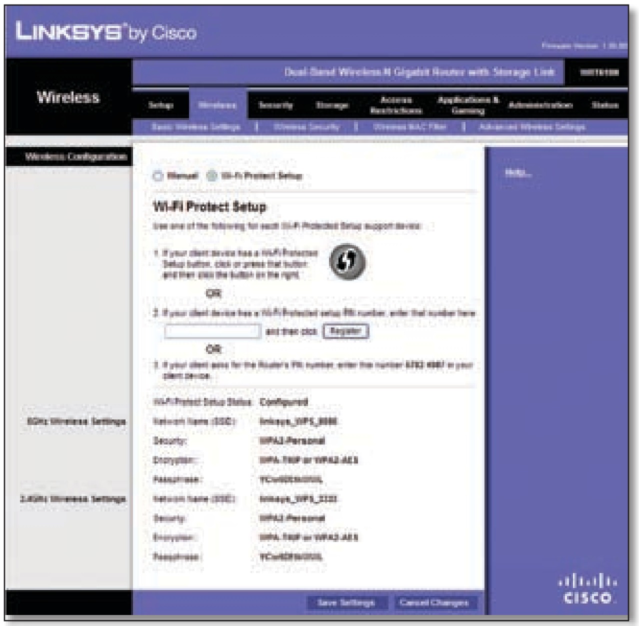
Standard Channel (2.4 GHz) Select the channel for Wireless-B, Wireless-G and Wireless-N (2.4GHz) networking. If you selected Wide – 40MHz Channel for the Radio Band setting, then the Standard Channel will be a secondary channel for Wireless-N (2.4GHz). If you are not sure which channel to select, keep the default, **Auto**.

SSID Broadcast When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the Router’s SSID, keep the default setting, **Enabled**. If you do not want to broadcast the Router’s SSID, then select **Disabled**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wi-Fi Protected Setup

There are three methods available. Use the method that applies to the client device you are configuring.



Wireless > Basic Wireless Settings (Wi-Fi Protected Setup)

NOTE: Wi-Fi Protected Setup configures one client device at a time. Repeat the instructions for each client device that supports Wi-Fi Protected Setup.

Method #1

Use this method if your client device has a Wi-Fi Protected Setup button.

1. Click or press the **Wi-Fi Protected Setup** button on the client device.
2. Click the **Wi-Fi Protected Setup** button on this screen.
3. After the client device has been configured, click the **OK** button. Then refer back to your client device or its documentation for further instructions.

Method #2

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

1. Enter the PIN number from the client device in the field on this screen.
2. Click the **Register** button.
3. After the client device has been configured, click the **OK** button. Then refer back to your client device or its documentation for further instructions.

Method #3

Use this method if your client device asks for the Router’s PIN number.

1. Enter the PIN number listed on this screen. (It is also listed on the label on the bottom of the Router.)
2. After the client device has been configured, click the **OK** button. Then refer back to your client device or its documentation for further instructions.

The Wi-Fi Protected Setup Status, Network Name (SSID), Security, Encryption, and Passphrase are displayed at the bottom of the screen.

NOTE: If you have client devices that do not support Wi-Fi Protected Setup, note the wireless settings, and then manually configure those client devices.

Wireless > Wireless Security

The Wireless Security settings configure the security of your wireless network. There are six wireless security mode options supported by the Router: WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS, and WEP. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption. WEP stands for Wired Equivalent Privacy, while RADIUS stands for Remote Authentication Dial-In User Service.) These six are briefly discussed here. For detailed information on setting up wireless security networks, refer to "Chapter 2: Wireless Security."

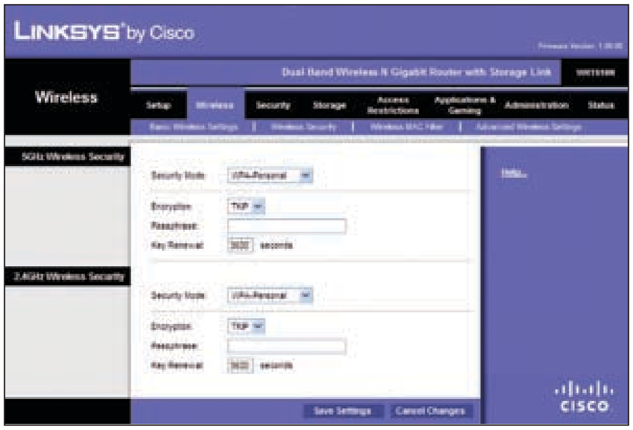
Wireless Security

Security Mode

Select the security method for your wireless network. If you do not want to use wireless security, keep the default, **Disabled**.

WPA Personal

NOTE: If you are using WPA or WPA2, each device in your wireless network MUST use the same WPA or WPA2 method and shared key, or else the network will not function properly.


LINKSYS by Cisco
Wireless
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
5GHz Wireless Security
2.4GHz Wireless Security
Help...
Save Settings
Cancel Changes
cisco

5GHz Wireless Security
Security Mode: WPA-Personal
Encryption: TKIP
Passphrase:
Key Renewal: 3600 seconds

2.4GHz Wireless Security
Security Mode: WPA-Personal
Encryption: TKIP
Passphrase:
Key Renewal: 3600 seconds

WPA Personal

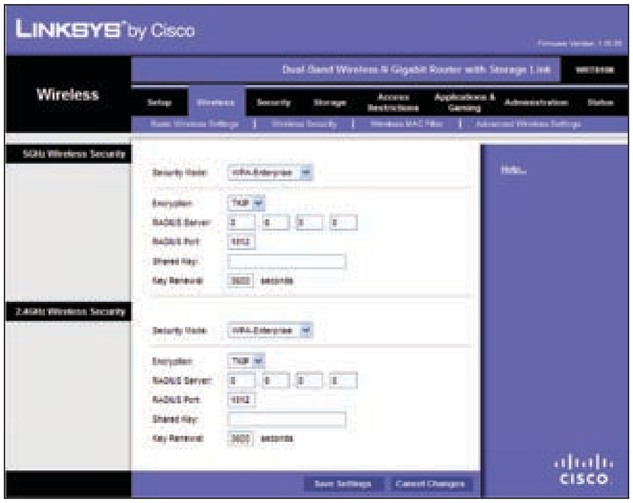
Encryption WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. The default is **TKIP**.

Passphrase Enter a passphrase of 8-63 characters.

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default Key Renewal period is **3600** seconds.

WPA Enterprise

This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)


LINKSYS by Cisco
Wireless
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
5GHz Wireless Security
2.4GHz Wireless Security
Help...
Save Settings
Cancel Changes
cisco

5GHz Wireless Security
Security Mode: WPA-Enterprise
Encryption: TKIP
RADIUS Server: 0 . 0 . 0 . 0
RADIUS Port: 1812
Shared Key:
Key Renewal: 3600 seconds

2.4GHz Wireless Security
Security Mode: WPA-Enterprise
Encryption: TKIP
RADIUS Server: 0 . 0 . 0 . 0
RADIUS Port: 1812
Shared Key:
Key Renewal: 3600 seconds

WPA Enterprise

Encryption WPA supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, **TKIP** or **AES**. The default is **TKIP**.

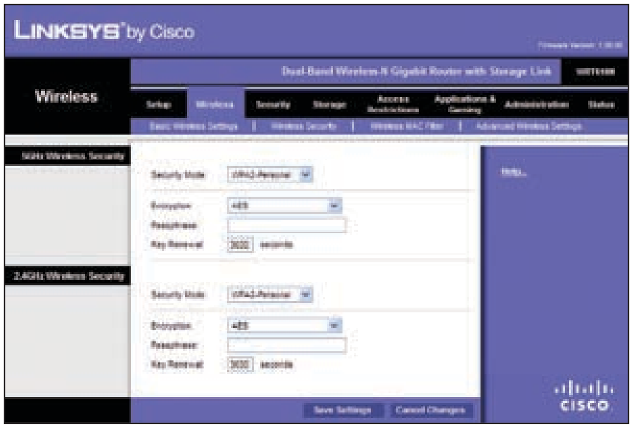
RADIUS Server Enter the IP Address of the RADIUS server.

RADIUS Port Enter the port number of the RADIUS server. The default value is **1812**.

Shared Key Enter the key shared between the Router and the server.

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default Key Renewal period is **3600** seconds.

WPA2 Personal


LINKSYS by Cisco
Dual-Band Wireless-N Gigabit Router with Storage Link
Wireless
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
5GHz Wireless Security
2.4GHz Wireless Security
Help...
Save Settings
Cancel Changes
cisco

5GHz Wireless Security
Security Mode: WPA2-Personal
Encryption: AES
Passphrase:
Key Renewal: 3600 seconds

2.4GHz Wireless Security
Security Mode: WPA2-Personal
Encryption: AES
Passphrase:
Key Renewal: 3600 seconds

WPA2 Personal

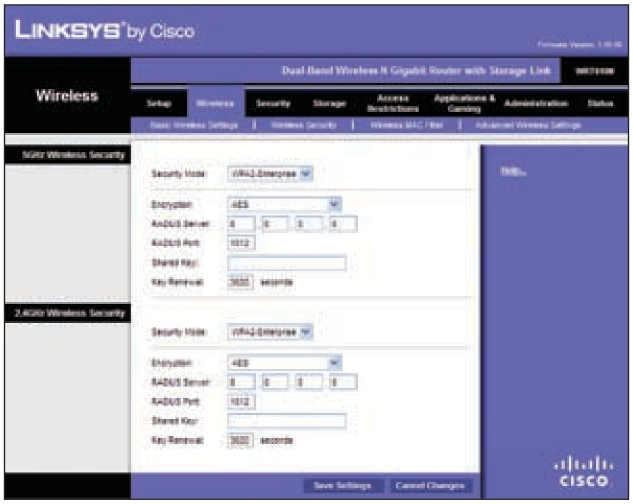
Encryption WPA2 supports two encryption methods with dynamic encryption keys; AES or WPA-TKIP/WPA2-AES. You must select **WPA-TKIP** or **WPA2-AES** to connect to the Router.

Passphrase Enter a passphrase of 8-63 characters.

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default Key Renewal period is **3600** seconds.

WPA2 Enterprise

This option features WPA2 used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)



WPA2 Enterprise

Encryption WPA2 supports two encryption methods with dynamic encryption keys; AES or WPA-TKIP/WPA2-AES. You must select **WPA-TKIP** or **WPA2-AES** to connect to the Router.

RADIUS Server Enter the IP Address of the RADIUS server.

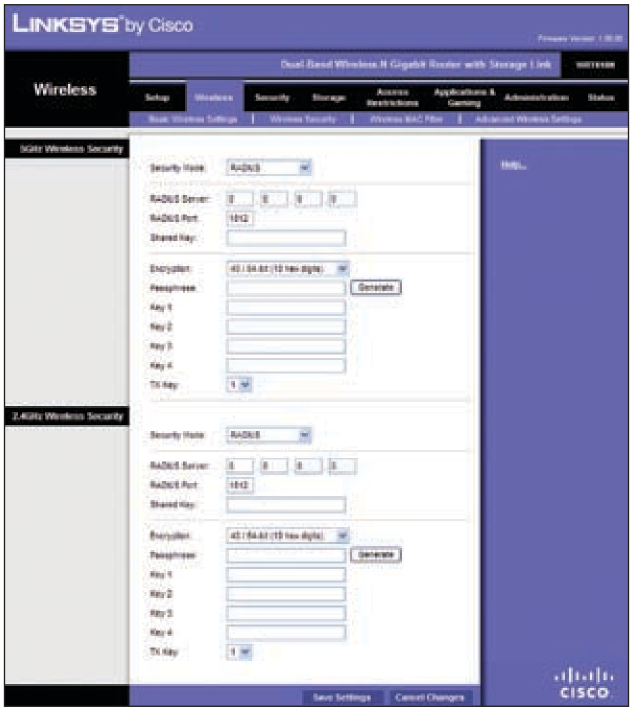
RADIUS Port Enter the port number of the RADIUS server. The default value is **1812**.

Shared Key Enter the key shared between the Router and the server.

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default Key Renewal time out period is **3600** seconds.

RADIUS

This option features WEP used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)



RADIUS

IMPORTANT: If you are using WEP encryption, always each device in your wireless network MUST use the same WEP encryption method and encryption key, or else your wireless network will not function properly.

RADIUS Server Enter the IP Address of the RADIUS server.

RADIUS Port Enter the port number of the RADIUS server. The default value is **1812**.

Shared Key Enter the key shared between the Router and the server.

Encryption Select a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. The default is **64 bits 10 hex digits**.

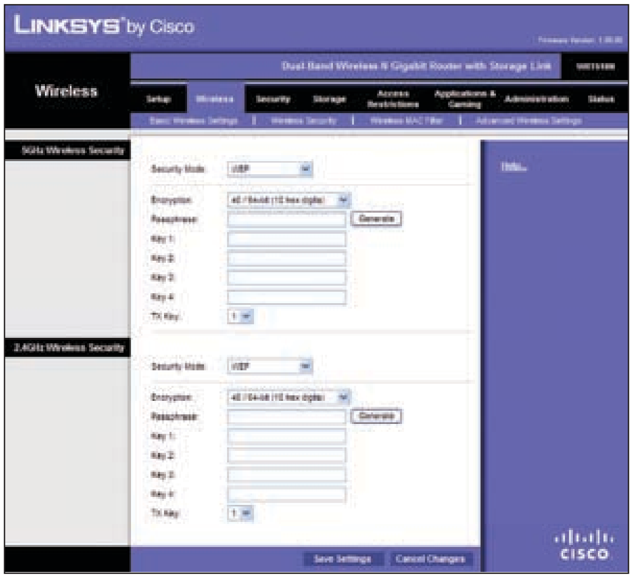
Passphrase Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.

Key 1-4 If you did not enter a Passphrase, enter the WEP key(s) manually.

Tx Key Select a key from the drop-down menu.

WEP

WEP is a basic encryption method that is not as secure as WPA.


LINKSYS by Cisco
Wireless
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
5GHz Wireless Security
Security Mode:
Encryption:
Passphrase:
Generate
Key 1:
Key 2:
Key 3:
Key 4:
TX Key:
2.4GHz Wireless Security
Security Mode:
Encryption:
Passphrase:
Generate
Key 1:
Key 2:
Key 3:
Key 4:
TX Key:
Help...
Save Settings
Cancel Changes
cisco

WEP

Encryption Select a level of WEP encryption, **64 bits 10 hex digits** or **128 bits 26 hex digits**. The default is **64 bits 10 hex digits**.

Passphrase Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.

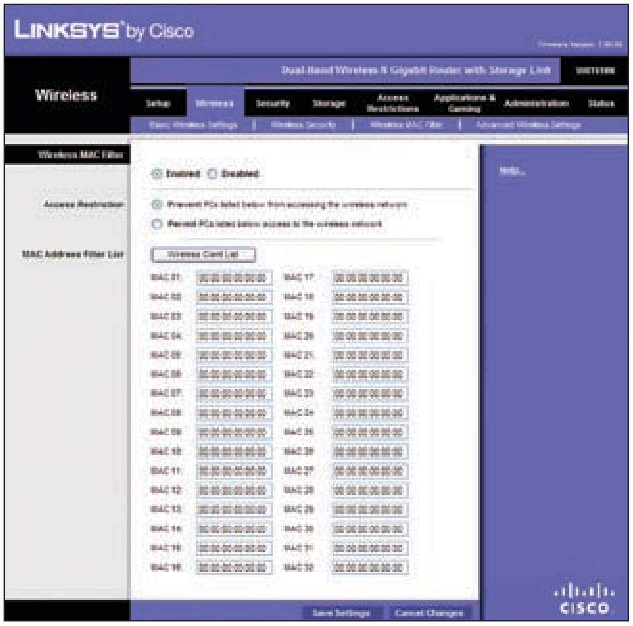
Key 1-4 If you did not enter a Passphrase, enter the WEP key(s) manually.

Tx Key Select a key from the drop-down menu.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wireless > Wireless MAC Filter

Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius.


LINKSYS by Cisco
Wireless
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Wireless MAC Filter
Enabled
Disabled
Access Restriction
MAC Address Filter List
Wireless Client List
Help...
Save Settings
Cancel Changes
cisco

Wireless > Wireless MAC Filter

Wireless MAC Filter

Access Restriction

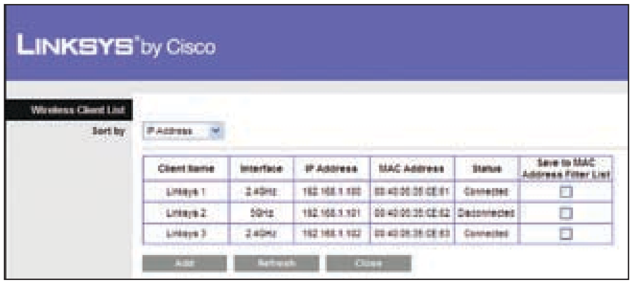
Wireless MAC Filter To filter wireless users by MAC Address, either permitting or blocking access, click **Enabled**. If you do not wish to filter users by MAC Address, keep the default setting, **Disabled**.

Prevent PCs listed below from accessing the wireless network Select this to block wireless access by MAC Address. This option is selected by default.

Permit PCs listed below to the wireless network Select this to allow wireless access by MAC Address. This option is not selected by default.

MAC Address Filter List

Click the **Wireless Client List** button to display the Wireless Client List. It shows computers and other devices on the wireless network. Click the **Save to MAC Address Filter List** checkbox for any device you want to add to the MAC Address Filter List. Then click the **Add** button. To retrieve the most up-to-date information, click the **Refresh** button. To exit this screen and return to the *Wireless MAC Filter* screen, click the **Close** button.



Sort by: IP Address

Client Name	Interface	IP Address	MAC Address	Status	Save to MAC Address Filter List
Linksys 1	2.4GHz	192.168.1.100	00:40:05:35:CE:61	Connected	☐
Linksys 2	5GHz	192.168.1.101	00:40:05:35:CE:62	Disconnected	☐
Linksys 3	2.4GHz	192.168.1.102	00:40:05:35:CE:63	Connected	☐

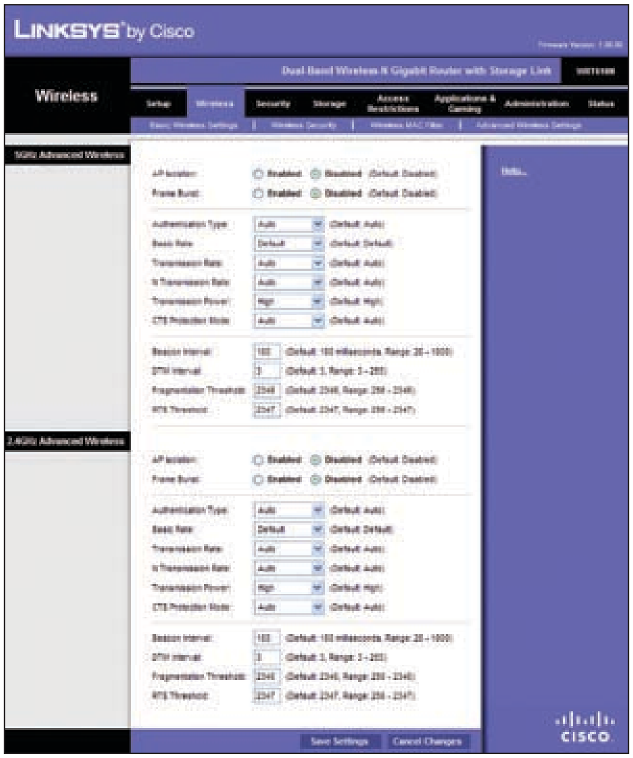
Wireless Client List

MAC XX Enter the MAC addresses of the devices whose wireless access you want to control.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wireless > Advanced Wireless Settings

This *Wireless > Advanced Wireless Settings* screen is used to set up the Router's advanced wireless functions. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.



5GHz Advanced Wireless

AP Isolation: ○ Enabled ● Disabled (Default: Disabled)
Frame Burst: ○ Enabled ● Disabled (Default: Disabled)
Authentication Type: Auto (Default: Auto)
Basic Rate: Default (Default: Default)
Transmission Rate: Auto (Default: Auto)
N Transmission Rate: Auto (Default: Auto)
Transmission Power: High (Default: High)
CTS Protection Mode: Auto (Default: Auto)
Beacon Interval: 100 (Default: 100 milliseconds, Range: 20 - 1000)
DTIM Interval: 3 (Default: 3, Range: 1 - 255)
Fragmentation Threshold: 2346 (Default: 2346, Range: 256 - 2346)
RTS Threshold: 2347 (Default: 2347, Range: 256 - 2347)

2.4GHz Advanced Wireless

AP Isolation: ○ Enabled ● Disabled (Default: Disabled)
Frame Burst: ○ Enabled ● Disabled (Default: Disabled)
Authentication Type: Auto (Default: Auto)
Basic Rate: Default (Default: Default)
Transmission Rate: Auto (Default: Auto)
N Transmission Rate: Auto (Default: Auto)
Transmission Power: High (Default: High)
CTS Protection Mode: Auto (Default: Auto)
Beacon Interval: 100 (Default: 100 milliseconds, Range: 20 - 1000)
DTIM Interval: 3 (Default: 3, Range: 1 - 255)
Fragmentation Threshold: 2346 (Default: 2346, Range: 256 - 2346)
RTS Threshold: 2347 (Default: 2347, Range: 256 - 2347)

Wireless > Advanced Wireless Settings

Advanced Wireless

AP Isolation This isolates all wireless clients and wireless devices on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, select **Enabled**. AP Isolation is disabled by default.

Frame Burst Enabling this option should provide your network with greater performance, depending on the manufacturer of your wireless products. To use the Frame Burst option, select **Disabled**. The default is **Enabled**.

Authentication Type The default is set to **Auto**, which allows either Open System or Shared Key authentication to be used. With **Open System** authentication, the sender and the recipient do NOT use a WEP key for authentication. With **Shared Key** authentication, the sender and recipient use a WEP key for authentication.

Basic Rate The Basic Rate setting is not one, but a series of rates at which the Router can transmit. (The Basic Rate is not the actual rate of data transmission. If you want to specify the Router's rate of data transmission, configure the Transmission Rate setting.) The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. The default setting is **Default**, when the Router can transmit at all standard wireless rates..

Transmission Rate The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is **Auto**.

CTS Protection Mode CTS (Clear-To-Send) Protection Mode should remain disabled unless you are having severe problems with your wireless products not being able to transmit to the Router in an environment with heavy latency wireless traffic. This function boosts the Router's ability to catch all wireless transmissions but will severely decrease performance. The default value is **Auto.**

Beacon Interval A beacon is a packet broadcast by the Router to synchronize the wireless network. Enter a value between 20 and 1000 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon.The default value is **100**.

DTIM Interval This value, between 3 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **3**.

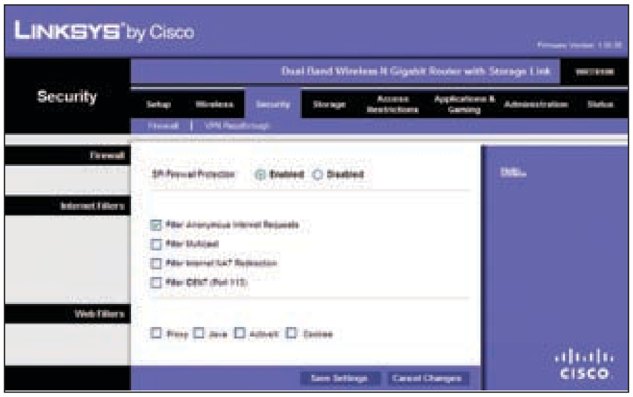
Fragmentation Threshold This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

RTS Threshold Should you encounter inconsistent data flow, only minor reduction of the default value, **2347**, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of **2347**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Security > Firewall

The *Security > Firewall* screen is used to configure a firewall that can filter out various types of unwanted traffic on the Router's local network.


LINKSYS by Cisco
Dual Band Wireless-N Gigabit Router with Storage Link
Security
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Firewall | VPN Passthrough
Firewall
Internet Filters
Web Filters
Help...
Save Settings
Cancel Changes
CISCO

SPI Firewall Protection ● Enabled ○ Disabled

☑ Filter Anonymous Internet Requests
☐ Filter Multicast
☐ Filter Internet NAT Redirection
☐ Filter IDENT (Port 113)

☐ Proxy ☐ Java ☐ ActiveX ☐ Cookies

Security > Firewall

Firewall

SPI Firewall Protection To use firewall protection, keep the default selection, **Enabled**. To turn off firewall protection, select **Disabled**.

Internet Filters

Filter Anonymous Internet Requests This feature makes it more difficult for outside users to work their way into your network. This feature is selected by default. Deselect the feature to allow anonymous Internet requests.

Filter Multicast Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, then the Router will allow IP multicast packets to be forwarded to the appropriate computers. It is selected by default. Deselect this feature to disable it.

Filter Internet NAT Redirection This feature is used to prevent a local computer from using a URL or Internet address to access the local server. Select **Filter Internet NAT Redirection** to filter Internet NAT redirection. It is not selected by default.

Filter IDENT (Port 113) This feature keeps port 113 from being scanned by devices outside of your local network. It is selected by default. Deselect this feature to disable it.

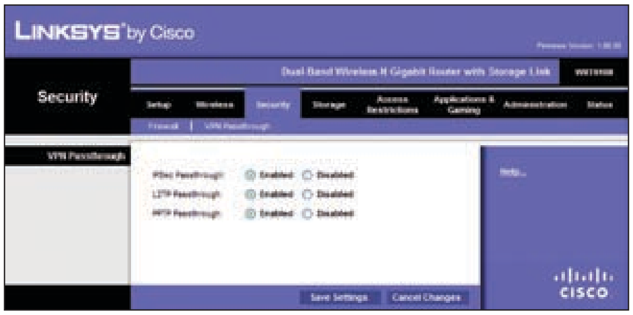
Web Filters

Filters Select to filter Proxy, Java, ActiveX, and Cookies.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Security > VPN Passthrough

The *Security > VPN Passthrough* screen allows you to enable VPN tunnels using IPSec, PPTP, or L2TP protocols to pass through the Router's firewall.


LINKSYS by Cisco
Dual Band Wireless-N Gigabit Router with Storage Link
Security
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Firewall | VPN Passthrough
VPN Passthrough
Help...
Save Settings
Cancel Changes
CISCO

IPSec Passthrough ● Enabled ○ Disabled
L2TP Passthrough ● Enabled ○ Disabled
PPTP Passthrough ● Enabled ○ Disabled

Security > VPN Passthrough

VPN Passthrough

IPSec Passthrough Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the Router, keep the default, **Enabled**.

PPTP Passthrough Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, keep the default, **Enabled**.

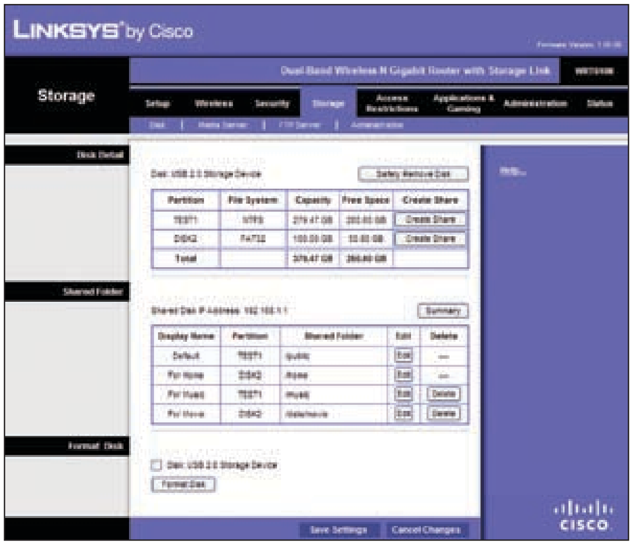
L2TP Passthrough Layer 2 Tunneling Protocol is the method used to enable Point-to-Point sessions via the Internet on the Layer 2 level. To allow L2TP tunnels to pass through the Router, keep the default, **Enabled**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Storage > Disk

An external USB hard drive or USB disk must be connected to the USB Port of the Router to use the storage feature.

The *Disk* screen describes the disk currently attached to the Router. Using this screen, you can format a blank disk, safely remove a disk, or erase a disk.


LINKSYS by Cisco
Storage
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Disk Detail
Shared Folder
Format Disk
Save Settings
Cancel Changes
CISCO

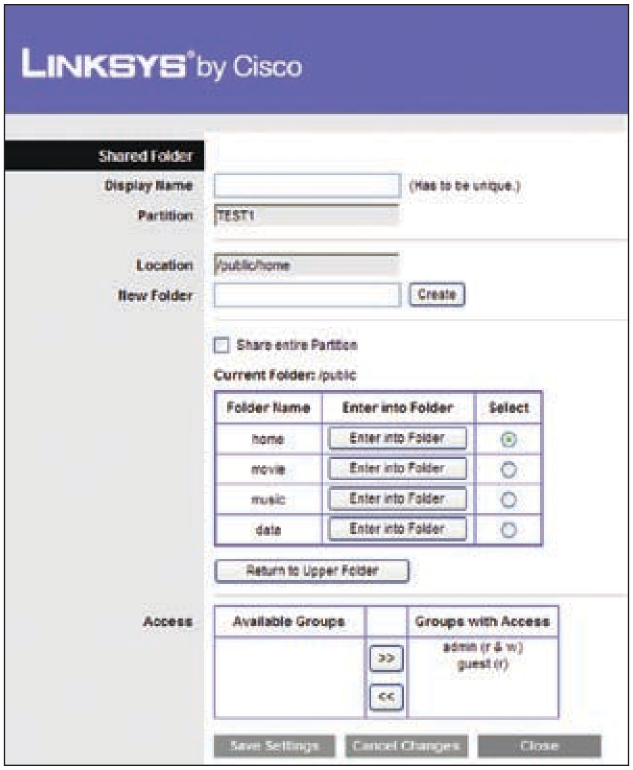
Storage > Disk

Disk Detail

If a formatted disk is attached to the Router, you can view the Partition, File System, Capacity, and Free Space information for each partition of the disk. Click **Create Share** to create a shared folder.

Safely Remove Disk Before physically disconnecting a disk from the Router, click **Safely Remove** first. This prevents the possible loss of data, if the disk is removed while data is transferring to or from the disk.

If you click **Create Share**, the *Shared Folder* screen appears.


LINKSYS by Cisco
Shared Folder
Create
Return to Upper Folder
>>
<<
Save Settings
Cancel Changes
Close

Display Name (Has to be unique.)

Partition TEST1

Location /public/home

New Folder

☐ Share entire Partition

Current Folder: /public

Folder Name	Enter into Folder	Select
home	Enter into Folder	●
movie	Enter into Folder	○
music	Enter into Folder	○
data	Enter into Folder	○

Access

Available Groups		Groups with Access
	>> <<	admin (r & w) guest (r)

Shared Folder Screen

Shared Folder Screen

Use this screen to add a Shared folder.

Display Name Enter a display name that will appear in the Shared Folder table of the *Disk* screen.

Partion The name of the Partion to share, that you selected in the *Shared Folder* will appear here.

Location The location of the shared folder is displayed.

New Folder To create a new folder, enter a name for the folder and click **Create**.

Share entire Partion To share the entire partition, click the check box for **Share entire Partion**.

If you don't want to share the entire partition, you can specify the folder you do want to share. Select a folder name to share. To see a sub-folder, click **Enter into Folder**. To return to the previous folder, click **Return to Upper Folder**. To create a new folder, enter a name in the *New Folder* field, then click **Create**.

Access Select the right Access arrows to allow access to a group or the left arrows to remove access to a group. You can allow Read and Write or Read Only access. To add more groups, go to the Storage > Administration s

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Close** to exit the screen.

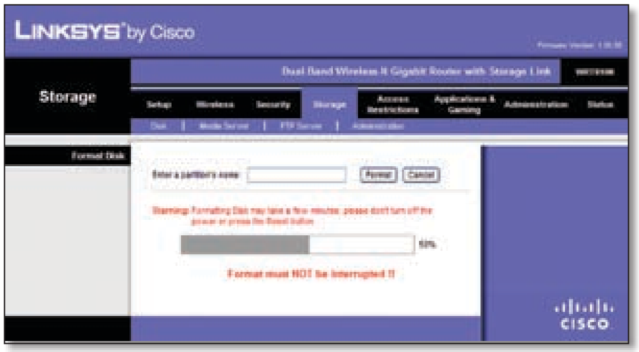
Shared Folder

Each Display Name you created on the *Shared Folder* screen will be listed with its partition and shared folder, which you can edit or delete. Select **Edit** to edit an item or **Delete** to delete the item.

If you click the **Edit**, the *Shared Folder* screen appears. Refer to the "Shared Folder Screen" section above.

Format Disk

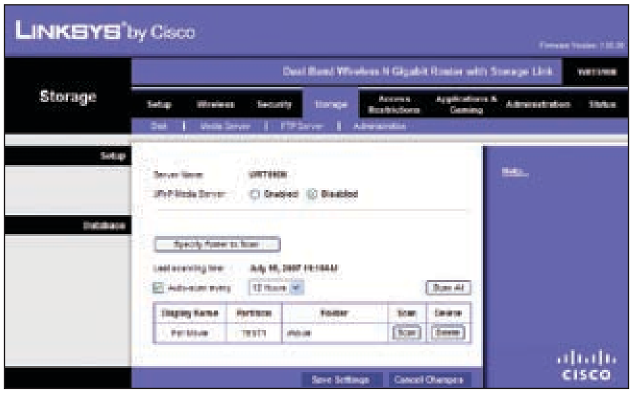
Select the disk you want to format, then click **Format Disk** to format the disk and create a new partition. If your hard drive is formatted with multiple partitions, it will delete them and create a single partition. Enter the name of the partition you want to format. Select **Format** to start the formatting or **Cancel** to cancel it before it begins.



Format Disk

Storage > Media Server

An external USB hard drive or USB disk must be connected to the USB Port of the Router to use the storage feature.



Storage > Media Server

Setup

Server Name The name of the router's media server is displayed here. It can be changed on the Storage > Administration screen.

UPnP Media Server To use the Router's media server function, select **Enabled**. Otherwise, select **Disabled**.

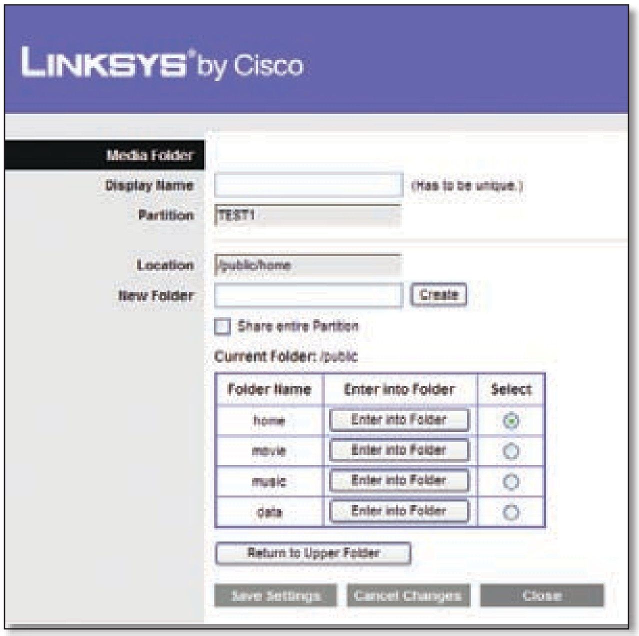
Database

This section lets you select content to add to the database of the Router's media server. Click **Specify Folder to Scan** to add a media folder to the Database table.

If you click **Specify Folder to Scan**, the *Media Folder* screen appears.

Media Folder Screen

Use this screen to add a Media folder.



Display Name (Has to be unique.)

Partition TEST1

Location /public/home

New Folder

☐ Share entire Partition

Current Folder: /public

Folder Name	Enter into Folder	Select
home	Enter into Folder	●
movie	Enter into Folder	○
music	Enter into Folder	○
data	Enter into Folder	○

Media Folder

Display Name Enter a display name that will appear in the Database table of the *Media Server* screen.

Partion The name of the Partion to share, that you selected in the *Shared Folder* will appear here.

Location The location of the shared folder is displayed.

New Folder To create a new folder, enter a name for the folder and click **Create**.

Share entire Partion To share the entire partition, click the check box for **Share entire Partion**.

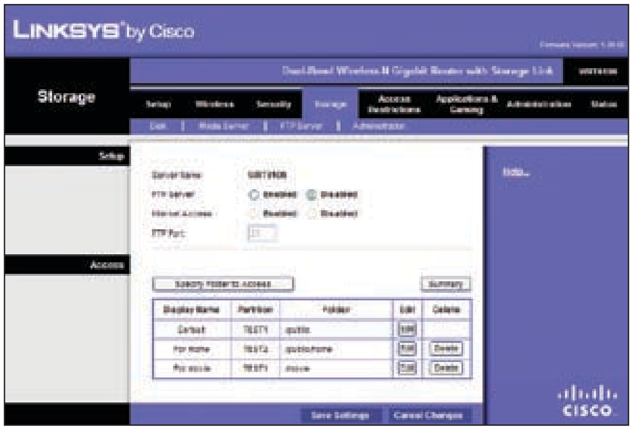
If you don't want to share the entire partition, you can specify the folder you do want to share. Select a folder name to share. To see a sub-folder, click **Enter into Folder**. To return to the previous folder, click **Return to Upper Folder**. To create a new folder, enter a name in the *New Folder* field, then click **Create**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. For more information, click **Help**.

Storage > FTP Server

An external USB hard drive or USB disk must be connected to the USB Port of the Router to use the storage feature.

The FTP Server tab creates an FTP Server that can be accessed from the Internet or your local network.


LINKSYS by Cisco
Storage
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Setup
Access
Save Settings
Cancel Changes
cisco

Storage> FTP Server

Setup

Server Name The name of the Router's FTP server is displayed here. It can be changed on the Storage > Administration screen.

FTP Server Select **Enabled** to set this Router as an FTP Server. Otherwise, select **Disabled** to turn the service off. An external USB hard drive or USB disk must be connected to the USB Port to use this service.

Internet Access Select **Enabled** to allow access of the FTP Server from the Internet. Otherwise, select **Disabled** to only allow local network access.

FTP Port Enter the FTP Port number to use. The default port is **21**.

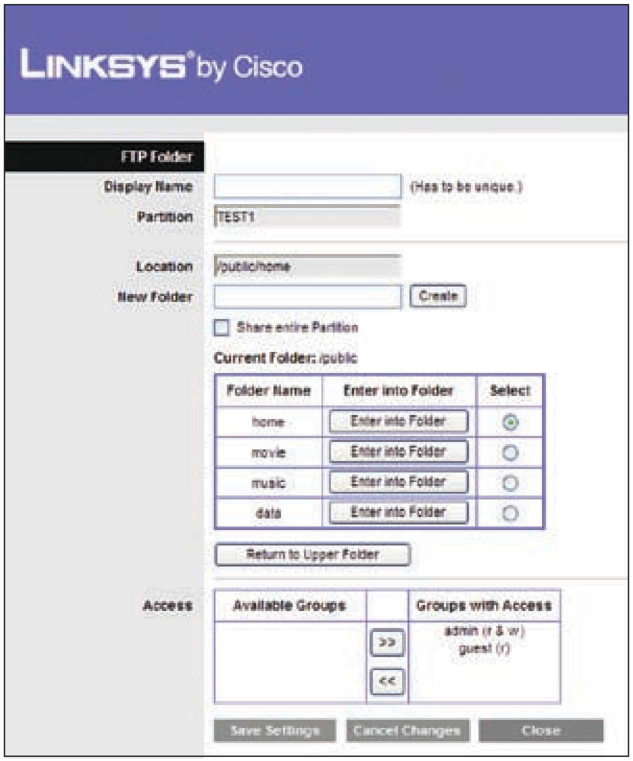
Access

This section lets you add FTP folders that can be accessed through the FTP client. Click **Specify Folder to Access** to add a FTP folder to the Access table.

If you click **Specify Folder to Access**, the *FTP Folder* screen appears.

FTP Folder Screen

Use this screen to add an FTP folder.


LINKSYS by Cisco
FTP Folder
Display Name
(Has to be unique.)
Partition
Location
New Folder
Create
Share entire Partition
Access
Available Groups
Groups with Access
>>
<<
Return to Upper Folder
Save Settings
Cancel Changes
Close

Partition: TEST1

Location: /public/home

☐ Share entire Partition

Current Folder: /public

Folder Name	Enter into Folder	Select
home	Enter into Folder	●
movie	Enter into Folder	○
music	Enter into Folder	○
data	Enter into Folder	○

Groups with Access: admin (r & w), guest (r)

FTP Folder Screen

Display Name Enter a display name that will appear in the Access table of the *FTP Server* screen.

Partion The name of the Partion to share, that you selected in the *Shared Folder* will appear here.

Location The location of the shared folder is displayed.

New Folder To create a new folder, enter a name for the folder and click **Create**.

Share entire Partion To share the entire partition, click the check box for **Share entire Partion**.

If you don't want to share the entire partition, you can specify the folder you do want to share. Select a folder name to share. To see a sub-folder, click **Enter into Folder**. To return to the previous folder, click **Return to Upper Folder**. To create a new folder, enter a name in the *New Folder* field, then click **Create**.

Access Select the right Access arrows to allow access to a group or the left arrows to remove access to a group. You can allow Read and Write or Read Only access. To add more groups, go to the Storage > Administration screen.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Close** to close the screen.

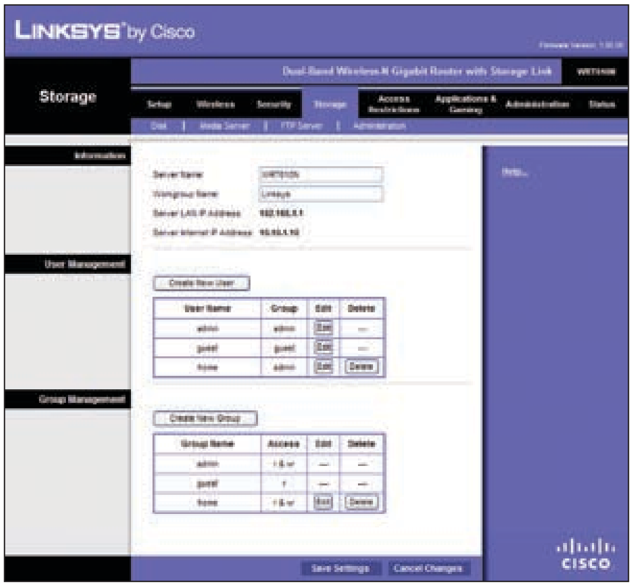
Each Display Name you created on the *FTP Folder* screen will be listed with its partition and folder, which you can edit or delete. Select **Edit** to edit an item or **Delete** to delete the item.

If you click **Edit**, the *FTP Folder* screen appears. Refer to the "FTP Folder Screen" section above.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. For more information, click **Help**.

Storage > Administration

The *Administration* screen allows you to manage the users and groups of users that can access the shares.



Storage > Administration

Information

Server Name Enter a name that will be used for the network storage FTP and Media server. Punctuation, spaces, and other special characters (e.g., * / | \) cannot be used in the name.

Workgroup Name Enter the Workgroup Name of your Router in the local network.

The (FTP and Media) Server LAN IP Address and the (FTP) Server Internet IP Address are displayed here.

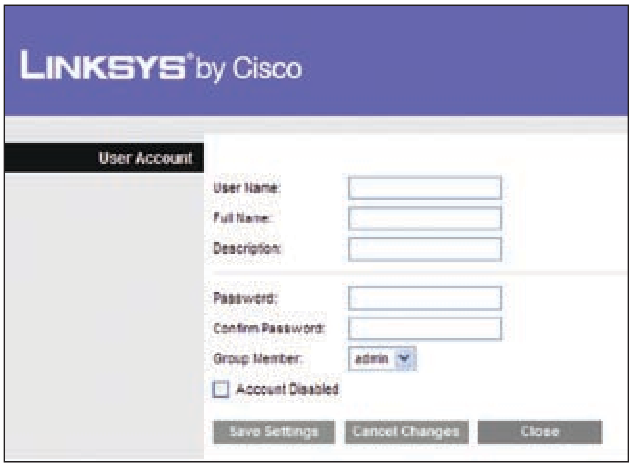
User Management

The available users are listed in the User Management table. The two default users, **Admin** (read and write access) and **Guest** (read-only access) cannot be deleted. Click **Create New User** to create a new user.

If you click **Create New User**, the *User Account* screen appears.

Each user you created on the *User Account* screen will be listed with its group, which you can edit or delete. Select **Edit** to edit a user or **Delete** to delete the user.

If you click **Edit**, the *User Account* screen appears. Refer to the "User Account Screen" section.



User Account

User Account Screen

Users can be added, edited or deleted through the *User Account* screen:

1. Enter a user name for the user.
2. Enter the full name and description for the user.
3. Enter a password and enter it again in the *Confirm Password* field.
4. Select **Admin** or **Guest** from the *Group Member* drop-down menu. You can create a new group in the Group Management section.
5. Click **Save Settings** to save the new changes, or click **Cancel Changes** to cancel the changes. Click **Close** to close the screen.

Group Management

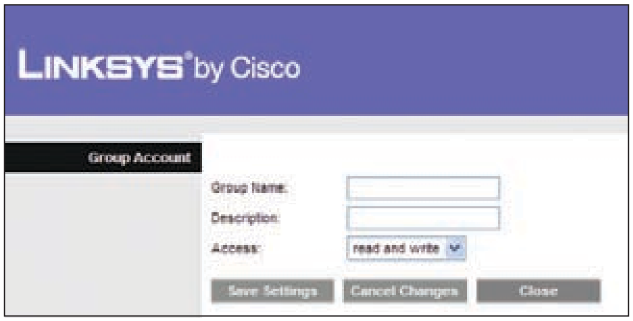
The groups are listed in the Group Management table. There are two default groups, **Admin** and **Guest**; these cannot be deleted. Click **Create New Group** to create a new group.

If you click **Create New Group**, the *Group Account* screen appears.

Each group you created on the *Group Account* screen will be listed with its access rights, which you can edit or delete. Select **Edit** to edit a user or **Delete** to delete the user.

If you click **Edit**, the *Group Account* screen appears. Refer to the "Group Account Screen" section.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. For more information, click **Help**.


LINKSYS® by Cisco
Group Account
Group Name:
Description:
Save Settings
Cancel Changes
Close

Access: read and write

Group Account

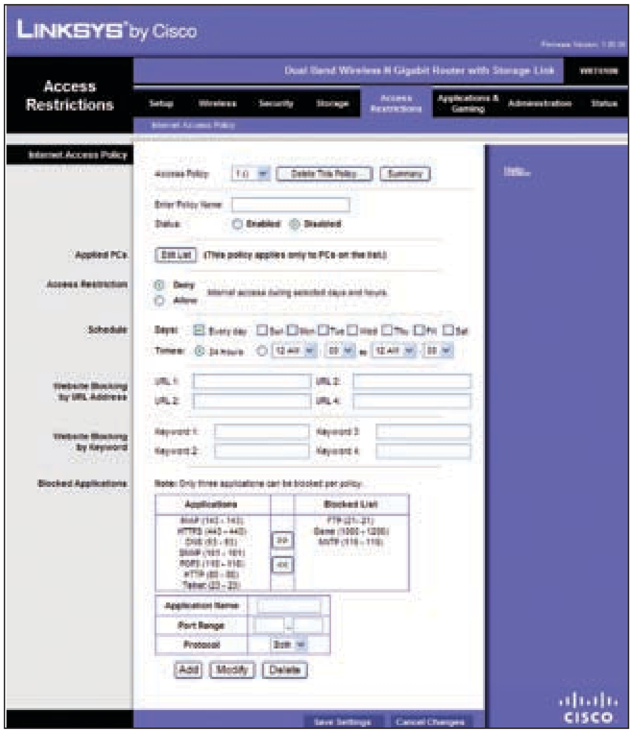
Group Account Screen

Groups can be added, edited or deleted:

1. Enter a name for the group.
2. Enter a description for the group.
3. Select **read and write** or **read only** access.
4. Click **Save Settings** to save the new changes, or click **Cancel Changes** to cancel the changes. Click **Close** to close the screen.

Access Restrictions > Internet Access

The *Access Restrictions > Internet Access* screen allows you to deny or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites during specific days and times.


LINKSYS® by Cisco
Access Restrictions
Dual Band Wireless-N Gigabit Router with Storage Link
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Internet Access Policy
Internet Access Policy
Access Policy:
Delete This Policy
Summary
Enter Policy Name:
Status:
Enabled
Disabled
Applied PCs:
Edit List
(This policy applies only to PCs on the list.)
Access Restriction:
Deny
Allow
Internet access during selected days and hours.
Schedule:
Days:
Everyday
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Times:
24 Hours
Website Blocking by URL Address
URL 1:
URL 2:
URL 3:
URL 4:
Website Blocking by Keyword
Keyword 1:
Keyword 2:
Keyword 3:
Keyword 4:
Blocked Applications
Note: Only three applications can be blocked per policy.
Applications
Blocked List
Application Name
Port Range
Protocol
Add
Modify
Delete
Help...
Save Settings
Cancel Changes
CISCO

Access Restrictions > Internet Access

Internet Access

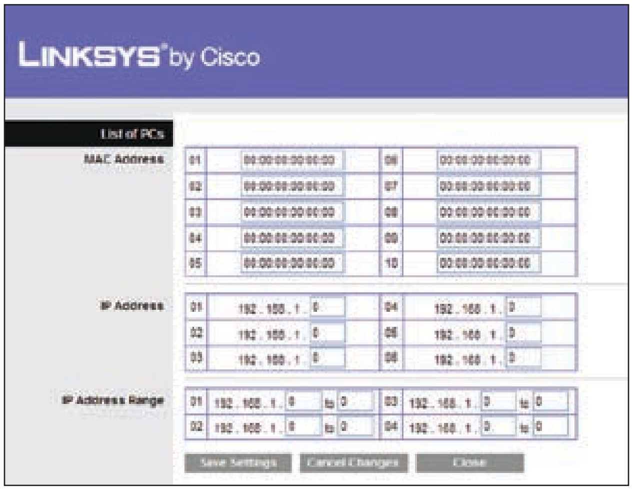
Internet Access Policy Internet Access can be managed by a policy. Use the settings on this screen to establish an access policy (after **Save Settings** is clicked). Selecting a policy from the drop-down menu will display that policy's settings. To delete a policy, select that policy's number and click **Delete**. To view all the policies, click **Summary**.

Deny or Allow If you select Deny, the PC on the Edit List will be denied Internet Access by the dates and times selected. PCs not on the list will still have Internet access. If you select Allow, the PCs on the Edit List will have Internet access by the dates and times selected. The PCs not on the Edit List will be denied Internet access. If there is a conflict with a policy, the lower numbered policy will have priority over a higher numbered policy.

To create an Internet Access Policy:

1. Select a number from the *Internet Access Policy* drop-down menu.
2. Enter a Policy Name in the field.
3. To enable this policy, select **Enabled**.

4. Click **Edit List of PCs** to select which PCs will be affected by the policy. The *List of PCs* screen appears. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want this policy to affect a group of PCs. After making your changes, click **Save Settings** to apply your changes or **Cancel Changes** to cancel your changes. Then click **Close**.


LINKSYS by Cisco
List of PCs
MAC Address
IP Address
IP Address Range
Save Settings
Cancel Changes
Close

MAC Address: 01–10 00:00:00:00:00:00

IP Address: 01–06 192.168.1.0

IP Address Range: 01–04 192.168.1.0 to 0

List of PCs

5. Select the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the *List of PCs* screen.
6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. Then enter a range of hours and minutes during which the policy will be in effect, or select **24 Hours**.
7. Enter a URL address or Keyword for Website Blocking or select any Blocked Applications you wish to use. Using these features can slow down your Internet speed.
8. Click **Save Settings** to save the policy's settings, or click **Cancel Changes** to cancel the policy's settings.

Blocked Applications

You can filter access to various services accessed over the Internet, such as FTP or telnet, by selecting applications from the Applications List.

To add an application, enter the application's name in the *Application Name* field. Enter its range in the *Port Range* fields. Select its protocol from the *Protocol* drop-down menu. Then click **Add**.

To modify an application, select it from the Application List. Change the application name, port range, or protocol setting. Then click **Modify**.

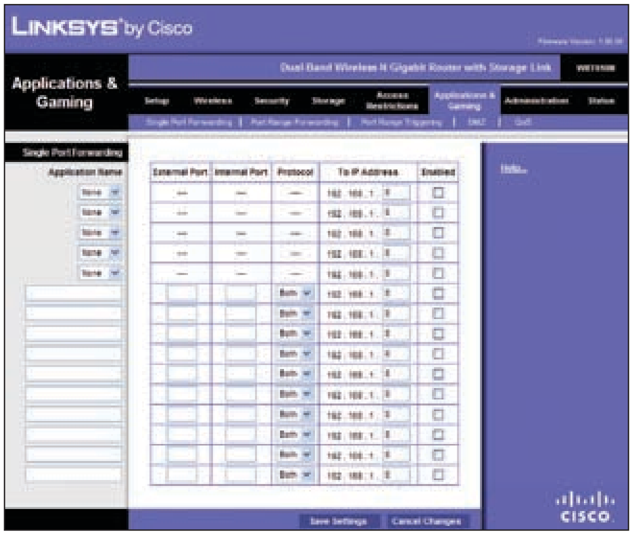
To delete an application, select it from the Application List. Then click **Delete**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications and Gaming > Single Port Forwarding

The *Single Port Forwarding* screen allows you to customize port services for common applications.

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers.


LINKSYS by Cisco
Applications & Gaming
Dual Band Wireless-N Gigabit Router with Storage Link
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Single Port Forwarding
Port Range Forwarding
Port Range Triggering
DMZ
QoS
Application Name
External Port
Internal Port
Protocol
To IP Address
Enabled
Help...
Save Settings
Cancel Changes
CISCO

Applications and Gaming > Single Port Forwarding

Single Port Forwarding

To forward a port, enter the information on each line for the criteria required.

Application Select a pre-configured application, or enter the name you wish to give the application. Each name can have up to 12 characters.

External and Internal Port Enter the external and internal port numbers.

Protocol Select the protocol used for this application, either **TCP** or **UDP**.

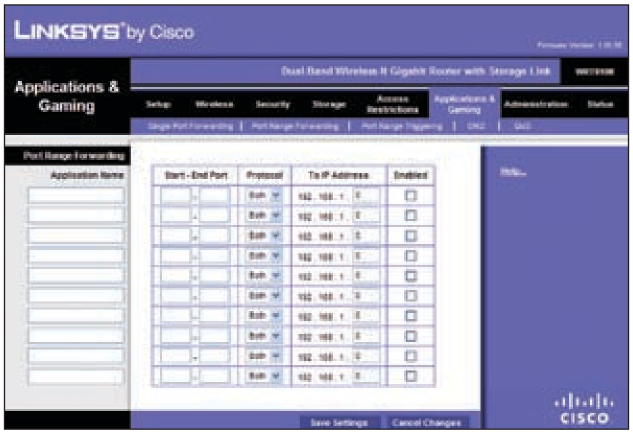
IP Address For each application, enter the IP address of the computer that should receive the requests.

Enabled For each application, select **Enabled** to enable port forwarding.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications and Gaming > Port Range Forwarding

The *Applications & Gaming > Port Range Forwarding* screen allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)


LINKSYS by Cisco
Dual-Band Wireless-N Gigabit Router with Storage Link
Applications & Gaming
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Single Port Forwarding | Port Range Forwarding | Port Range Triggering | DMZ | QoS
Port Range Forwarding
Application Name
Start - End Port
Protocol
To IP Address
Enabled
Both
192 . 168 . 1 .
Help...
Save Settings
Cancel Changes
CISCO

Applications and Gaming > Port Range Forwarding

Port Range Forwarding

To forward a port, enter the information on each line for the criteria required.

Application In this field, enter the name you wish to give the application. Each name can be up to 12 characters.

Start/End This is the port range. Enter the number that starts the port range in the Start column and the number that ends the range in the End column.

Protocol Select the protocol used for this application, either **TCP** or **UDP**, or **Both**.

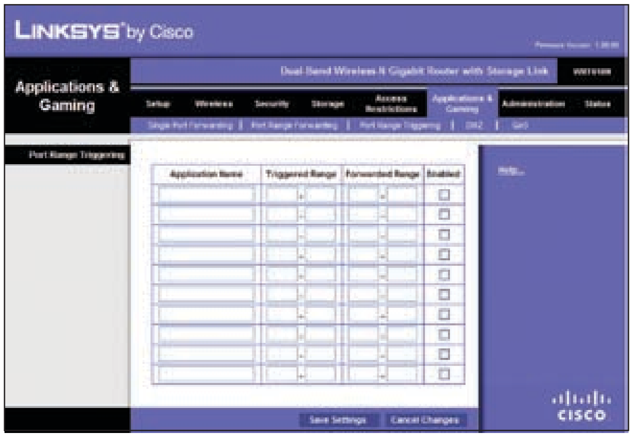
IP Address For each application, enter the IP Address of the PC running the specific application.

Enabled Select **Enabled** to enable port forwarding for the relevant application.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications & Gaming > Port Triggering

The *Applications & Gaming > Port Triggering* screen allows the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.


LINKSYS by Cisco
Dual-Band Wireless-N Gigabit Router with Storage Link
Applications & Gaming
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Single Port Forwarding | Port Range Forwarding | Port Range Triggering | DMZ | QoS
Port Range Triggering
Application Name
Triggered Range
Forwarded Range
Enabled
Help...
Save Settings
Cancel Changes
CISCO

Applications and Gaming > Port Triggering

Port Triggering

Application Enter the application name of the trigger.

Triggered Range

For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed.

Start Port Enter the starting port number of the Triggered Range.

End Port Enter the ending port number of the Triggered Range.

Forwarded Range

For each application, list the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.

Start Port Enter the starting port number of the Forwarded Range.

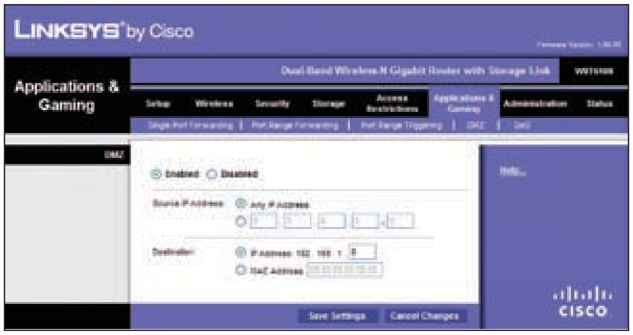
End Port Enter the ending port number of the Forwarded Range.

Enabled Select **Enabled** to enable port triggering for the applicable application.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications and Gaming > DMZ

The DMZ feature allows one network computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Forward feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet.



Applications and Gaming > DMZ

DMZ

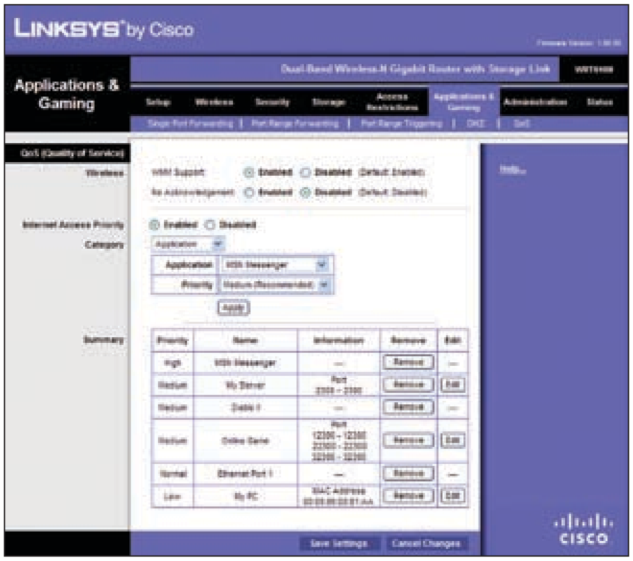
Any PC whose port is being forwarded should have its DHCP client function disabled and have a new static IP address assigned to it because its IP address may change when using the DHCP function.

To allow PCs on the Internet to access a local PC, select **Enabled**. Then, select **Any IP Address** or manually enter a specific source IP address of the computer you want to allow access from the Internet. Then, enter your local PC's IP address or MAC address that you want to allow access to. This feature is disabled by default.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications and Gaming > QoS

Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing.



Applications and Gaming > QoS

QoS (Quality of Service)

Wireless

Wireless WMM (Wi-Fi Multimedia) WMM is a wireless Quality of Service feature that improves quality for audio, video, and voice applications by prioritizing wireless traffic. To use this feature, your wireless client devices in your network must support Wireless WMM. If you would like to disable this feature, select **Disabled**. Otherwise, keep the default, **Enabled**.

No Acknowledgement If you want to disable the Router's Acknowledgement feature, so the Router will not re-send data if an error occurs, select **Enabled**. Otherwise, keep the default, **Disabled**.

Internet Access Priority

In this section, you can set the bandwidth priority for a variety of applications and devices. There are four levels of priority; High, Medium, Normal, or Low. When you set priority, do not set all applications to High, because this will defeat the purpose of allocating the available bandwidth. If you want to select below normal bandwidth, select Low. Depending on the application, a few attempts may be needed to set the appropriate bandwidth priority.

Enabled/Disabled To use the QoS policies you set, select **Enabled**. Otherwise, select **Disabled**.

Category

There are four categories available. Select one of the following: Applications, Online Games, MAC Address, Ethernet Port, or Voice Device. Proceed to the instructions for your selection.

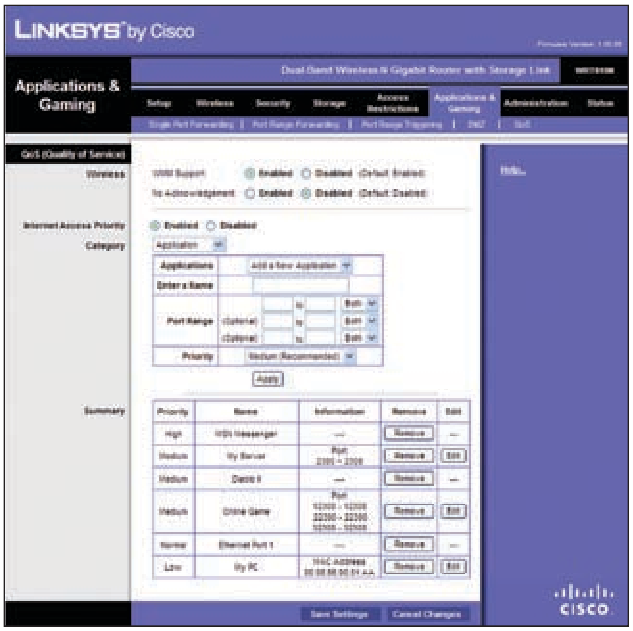
Applications

Applications Select the appropriate application. If you select *Add a New Application*, follow the instructions in the "Add a New Application "section.

Priority Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Add a New Application



Add a New Application

Enter a Name Enter a name for this application.

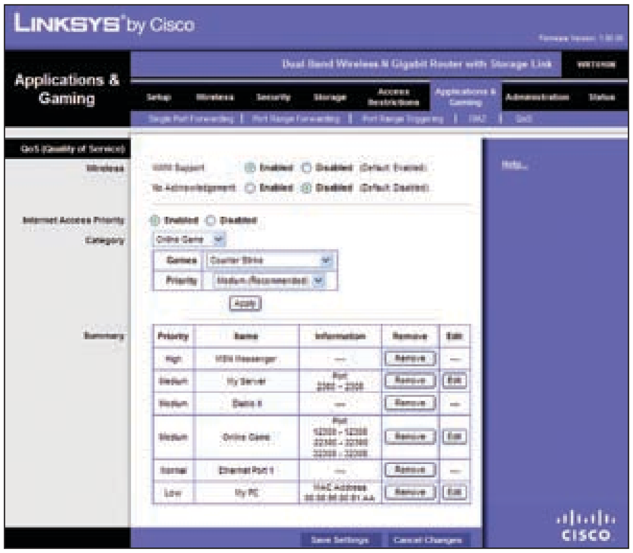
Port Range Enter the port range that the application will be using. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an application that uses from 1000 to 1250, you enter 1000-1250 as your settings. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used.

Select the protocol **TCP** or **UDP,** or select **Both**.

Priority Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Online Games



Online Games

Games

Games Select the appropriate game. If you select *Add a New Game*, follow the instructions in the "Add a New Game section".

Priority Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Add a New Game

Enter a Name Enter any name to indicate the name of the entry.

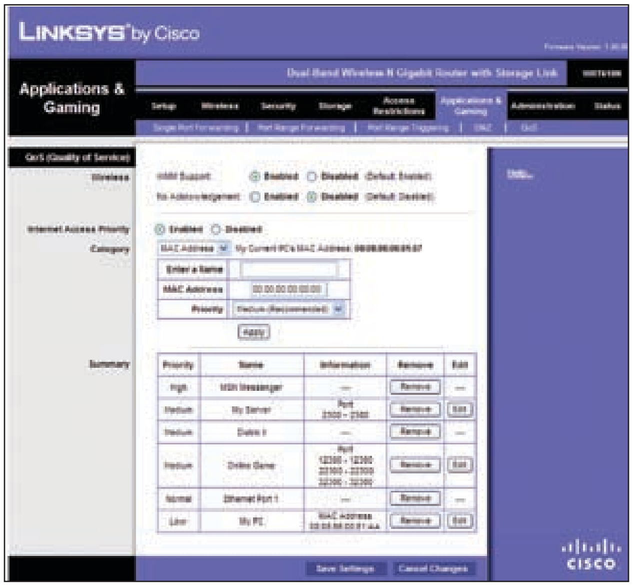
Port Range Enter the port range that the application will be using. For example, if you want to allocate bandwidth for FTP, you can enter 21-21. If you need services for an application that uses from 1000 to 1250, you enter 1000-1250 as your settings. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535. Check your application's documentation for details on the service ports used.

Select the protocol **TCP** or **UDP,** or select **Both**.

Priority Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

MAC Address



MAC Address

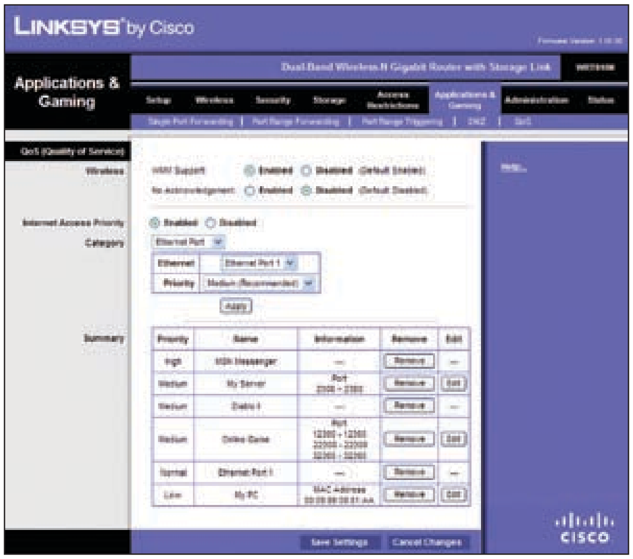
Enter a Name Enter a name for your device.

MAC Address Enter the MAC address of your device.

Priority Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the *Summary* list.

Ethernet Port



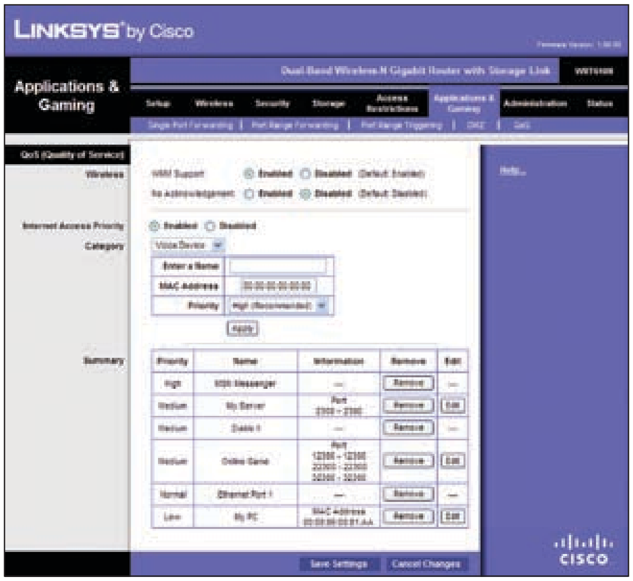
Ethernet Port

Ethernet Select the Ethernet port that you want to use.

Priority Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Voice Device



Voice Device

Enter a Name Enter a name for your voice device.

MAC Address. Enter the MAC address of your voice device.

Priority Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.

Click **Add** to save your changes. Your new entry will appear in the Summary list.

Summary

This lists the QoS entries you have created for your applications and devices.

Priority This displays the bandwidth priority of High, Medium, Normal, or Low.

Name This displays the application, device, or port name.

Information This displays the port range or MAC address entered for your entry. If a pre-configured application or game was selected, there will be no valid entry shown in this section.

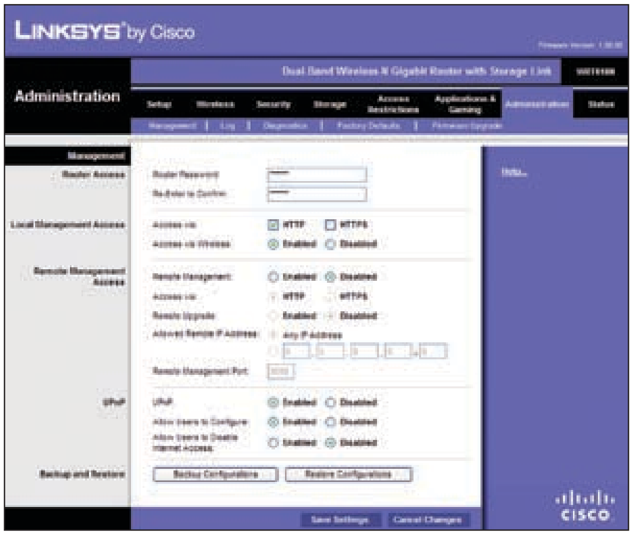
Remove Click this button to remove an entry.

Edit Click this button to make changes.

When you finish making changes to this screen, click **Save Settings** to save the changes, or click **Cancel Changes** to undo your changes. For more information, click **Help**.

Administration > Management

The *Administration > Management* screen allows the network's administrator to manage specific Router functions for access and security.



Administration > Management

Router Password

Router Access

Router Password Enter a new Password for the Router.

Re-enter to confirm Enter the Password again to confirm.

Local Management Access

Access via HTTP (HyperText Transport Protocol) is the communications protocol used to connect to servers on the World Wide Web. HTTPS uses SSL (Secured Socket Layer) to encrypt data transmitted for higher security. Select the **HTTP** or **HTTPS** check box. The default selection is **HTTP**.

Access via Wireless If you are using the Router in a public domain where you are giving wireless access to your guests, you can disable wireless access to the Router's web-based utility. You will only be able to access the web-based utility via a wired connection if you disable the setting. Keep the default, **Enabled**, to enable wireless access to the Router's web-based utility, or select **Disabled** to disable wireless access to the utility.

Remote Management Access

Remote Management To access the Router remotely from the Internet, select **Enabled**.

Access via Select **HTTP** or **HTTPS** communications protocols for remote access from the Internet.

Remote Upgrade Select **Enabled** to be able to upgrade the firmware remotely from the Internet.

Allowed Remote IP Address Select **Any IP Address** or manually enter an Internet IP address to allow remote access to the web-based utility from the Internet.

Remote Management Port Enter the port number that will provide outside access to the Router's web-based utility. You will need to enter the Router's password when accessing the Router this way, as usual.

UPnP

UPnP Keep the default, **Enabled**, to enable the UPnP feature; otherwise, select **Disabled**.

Allow Users to Configure To use the Allow Users to Configure UPnP options from the Windows operating system, select **Enabled**.

Allow Users to Disabled Internet Access To use the Allow Users to Disabled Internet Access options from the Windows operating system, click **Disabled**.

Backup and Restore

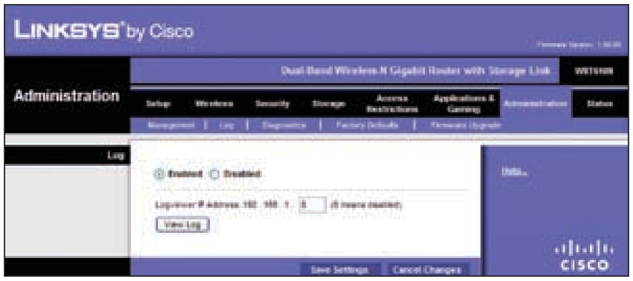
Backup Configurations To back up the Router's configuration file, click this button. Then, follow the on-screen instructions.

Restore Configurations To restore the Router's configuration file, click this button. Then, follow the on-screen instructions.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Administration > Log

The Router can keep logs of all traffic for your Internet connection.



Administration > Log

Log

Log To disable the Log function, keep the default setting, **Disabled**. To monitor traffic between the network and the Internet, select **Enabled**.

Logviewer IP Address If your computer uses Logviewer software you can enter enter the fixed IP address of the PC running the software in the Logviewer IP Address field.s The Router will now send updated logs to that PC.

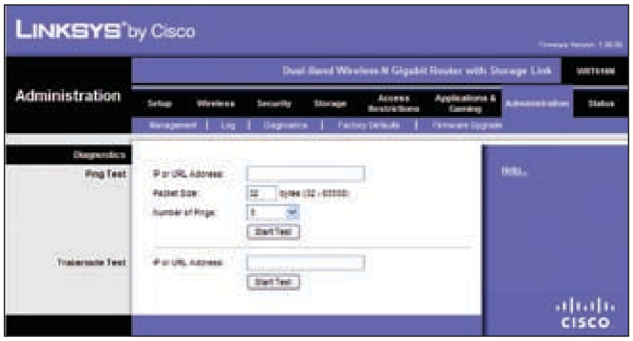
When you wish to view the logs, click **View Log**.

Click **Save the Log** to save your log, click **Refresh** to refresh the screen, or click **Clear** to clear the screen.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Administration > Diagnostics

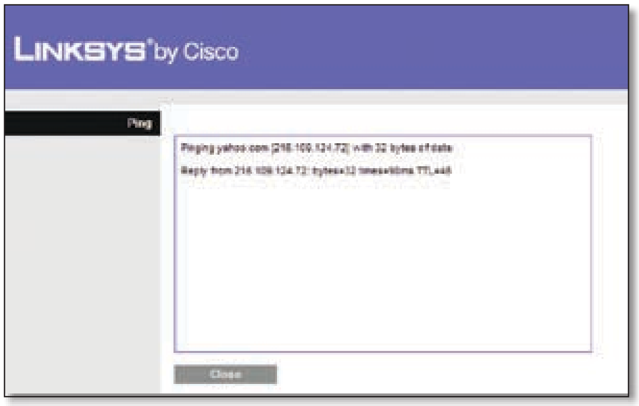
The diagnostic tests (Ping and Traceroute) allow you to check the connections of your Internet network.



Administration > Diagnostics

Ping Test

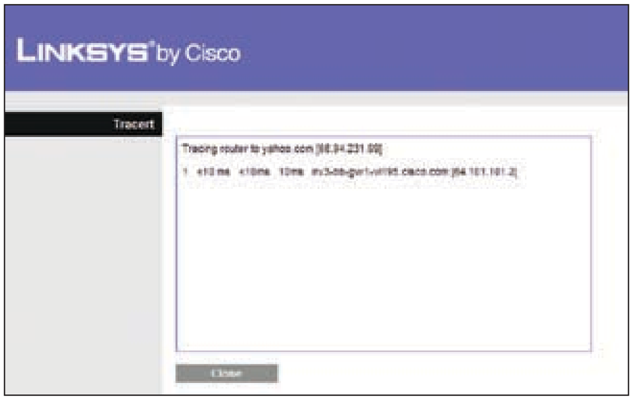
Ping The Ping test checks the status of a connection. Enter the address of the PC whose connection you wish to test and how many times you wish to test it. Then, click **Start to Ping**. The *Ping Test* screen will show if the test was successful. Click **Close** to return to the *Diagnostics* screen.



Ping Test

Traceroute Test

Traceroute To test the performance of a connection, click **Traceroute** to open the *Traceroute Test* screen. Enter the address of the PC whose connection you wish to test and click **Traceroute**. The *Traceroute Test* screen will show if the test was successful. Click **Close** to return to the *Diagnostics* screen.



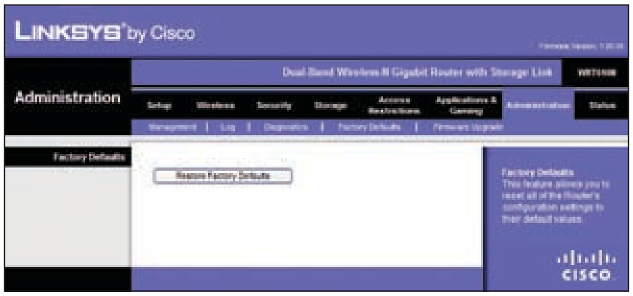
Traceroute Test

Administration > Factory Defaults

The *Administration > Factory Defaults* screen allows you to restore the Router's configuration to its factory default settings.

Factory Defaults

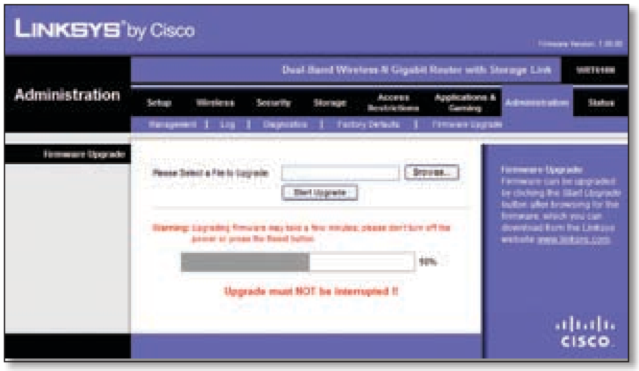
Restore Factory Defaults To reset the Router's settings to the default values, select **Restore Factory Defaults**. Any settings you have saved will be lost when the default settings are restored.



Administration > Factory Defaults

Administration > Firmware Upgrade

The *Administration > Firmware Upgrade* screen allows you to upgrade the Router's firmware. Do not upgrade the firmware unless you are experiencing problems with the Router or the new firmware has a feature you want to use.


LINKSYS by Cisco
Administration
Dual-Band Wireless-N Gigabit Router with Storage Link
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Firmware Upgrade
Browse...
Start Upgrade
Upgrade must NOT be interrupted !!
CISCO

Administration > Firmware Upgrade

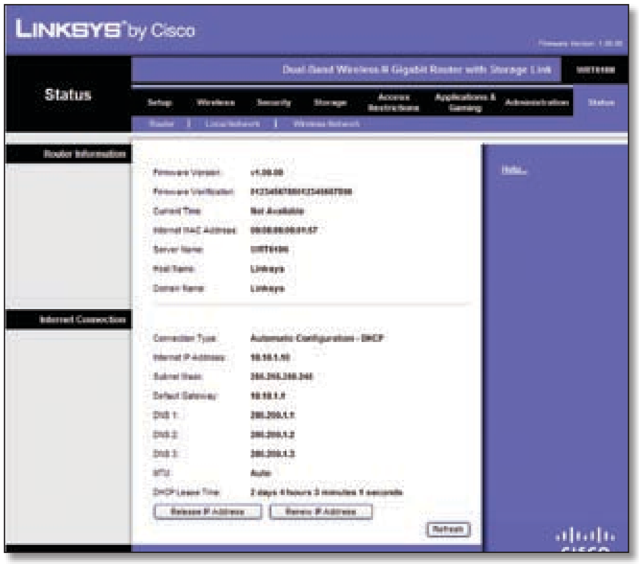
Before upgrading the firmware, download the Router's firmware upgrade file from the Linksys website, www.linksys.com. Then extract the file.

Upgrade Firmware

Please select a file to upgrade Click **Browse** and select the extracted firmware upgrade file. Then click **Upgrade** and follow the on-screen instructions.

Status > Router

The *Status* > *Router* screen displays the Router's current status.


LINKSYS by Cisco
Status
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Router Information
Internet Connection
Release IP Address
Renew IP Address
Refresh

Status > Router

Router Information

Firmware Version This is the Router's current firmware.

Firmware Verification This is a unique identifer that verifies that you have valid firmware.

Current Time This shows the time, as you set on the *Setup* tab.

Internet MAC Address This is the Router's MAC Address, as seen by your ISP.

Server Name This is the specific name that will be used for the network storage FTP and Media Server. You entered this name on the *Storage > Administration* tab.

Host Name If required by your ISP, this would have been entered on the *Setup* tab.

Domain Name If required by your ISP, this would have been entered on the *Setup* tab.

Internet Connection

Connection Type

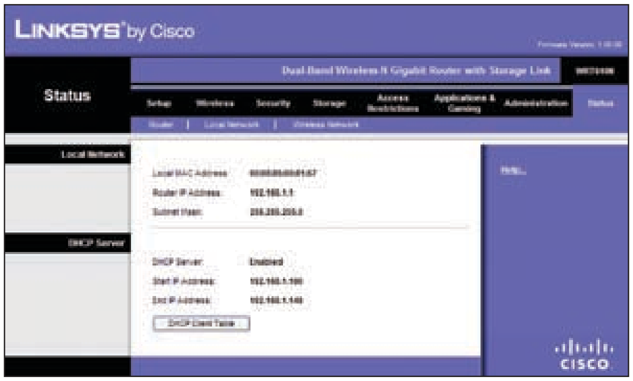
This section shows the current network information stored in the Router. The information varies depending on the Internet connection type selected on the *Setup > Basic Setup* screen.

Select **Release IP Address** or **Renew IP Address** as appropriate to release or renew a DHCP lease.

Click **Refresh** to update the on-screen information.

Status > Local Network

The *Status* > *Local Network* screen displays information about the local network.


LINKSYS by Cisco
Status
Setup
Wireless
Security
Storage
Access Restrictions
Applications & Gaming
Administration
Status
Local Network
DHCP Server
DHCP Client Table
CISCO

Status > Local Network

Local Network

Local MAC Address The MAC Address of the Router's local interface is displayed here.

Router IP Address This shows the Router's IP address, as it appears on your local network.

Subnet Mask The Router's Subnet Mask is shown here.

DHCP Server The status of the Router's DHCP server function is displayed here.

Start IP Address For the range of IP addresses used by devices on your local network, the beginning IP address is shown here.

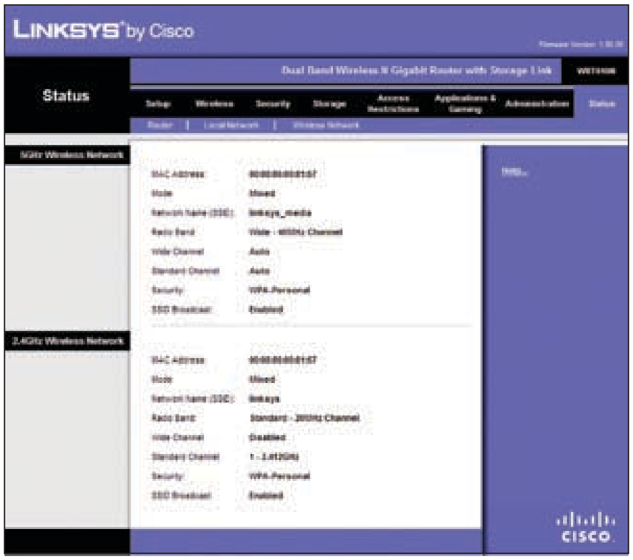
End IP Address For the range of IP addresses used by devices on your local network, the ending IP address is shown here.

DHCP Client Table Click **DHCP Client Table** to view the DHCP Client Table. It lists computers and other devices that have been assigned IP addresses by the Router.

For more information, click **Help**.

Status > Wireless Network

The *Status > Wireless Network* screen displays the status information of your 5 GHz and/or 2.4 GHz wireless networks.



Status > Wireless Network

5GHz/2.4GHz Wireless Network

MAC Address The MAC Address of the Router's wireless interface is displayed here.

Mode The wireless mode (Mixed, Wireless-N Only, Wireless-G Only, Wireless-B Only, Wireless-A Only or Disabled) used by the network is displayed here.

Net work Name (SSID) The name of the wireless network or SSID is displayed here.

Radio Band The Radio Band setting selected on the *Basic Wireless Settings* screen is displayed here.

Wide Channel The Wide Channel setting selected on the *Basic Wireless Settings* screen is displayed here.

Standard Channel The Standard Channel setting selected on the *Basic Wireless Settings* screen is displayed here.

Security The wireless security method used by the Router is displayed here.

SSID Broadcast The status of the SSID Broadcast feature is displayed here.

For more information, click **Help**.

Appendix A: Troubleshooting

Your computer cannot connect to the Internet.

Follow these instructions until your computer can connect to the Internet:

- Make sure that the Router is powered on. The Power LED should be green and not flashing.
- If the Power LED is flashing, then power off all of your network devices, including the modem, Router, and computers. Then power on each device in the following order:
    1. Cable or DSL modem
    2. Router
    3. Computer
- Check the cable connections. The computer should be connected to one of the ports numbered 1-4 on the Router, and the modem must be connected to the Internet port on the Router.

The modem does not have an Ethernet port.

The modem is a dial-up modem for traditional dial-up service. To use the Router, you need a cable/DSL modem and high-speed Internet connection.

You cannot use the DSL service to connect manually to the Internet.

After you have installed the Router, it will automatically connect to your Internet Service Provider (ISP), so you no longer need to connect manually.

The DSL telephone line does not fit into the Router's Internet port.

The Router does not replace your modem. You still need your DSL modem in order to use the Router. Connect the telephone line to the DSL modem, and then insert the setup CD into your computer. Click **Setup** and follow the on-screen instructions.

When you double-click the web browser, you are prompted for a username and password. If you want to get rid of the prompt, follow these instructions.

Launch the web browser and perform the following steps (these steps are specific to Internet Explorer but are similar for other browsers):

1. Select **Tools** > **Internet Options**.
2. Click the **Connections** tab.
3. Select **Never dial a connection**.
4. Click **OK**.

The Router does not have a coaxial port for the cable connection.

The Router does not replace your modem. You still need your cable modem in order to use the Router. Connect your cable connection to the cable modem, and then insert the setup CD into your computer. Click **Setup** and follow the on-screen instructions.

The computer cannot connect wirelessly to the network.

Make sure the wireless network name or SSID is the same on both the computer and the Router. If you have enabled wireless security, then make sure the same security method and key are used by both the computer and the Router.

You need to modify the settings on the Router.

Open the web browser (for example, Internet Explorer or Firefox), and enter the Router's IP address in the address field (the default IP address is **192.168.1.1**). When prompted, enter the password to the Router (the default is **admin**). Click the appropriate tab to change the settings.

WEB: If your questions are not addressed here, refer to the Linksys website, **www.linksys.com**

Appendix B: How to Install and Access USB Storage

Overview

This appendix explains how to connect and access an external USB storage device.

How to Install the USB Storage

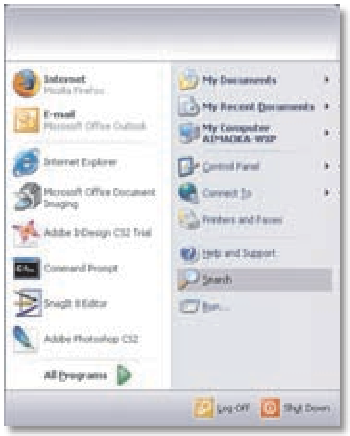
1. Make sure your computer has a wired or wireless connection to the Router.
2. Connect an external USB hard drive or USB flash disk to the USB port of the Router.
3. Proceed to the next section, "How to Access the USB Storage".

How to Access the USB Storage

Follow the instructions for your Windows operating system, XP or Vista.

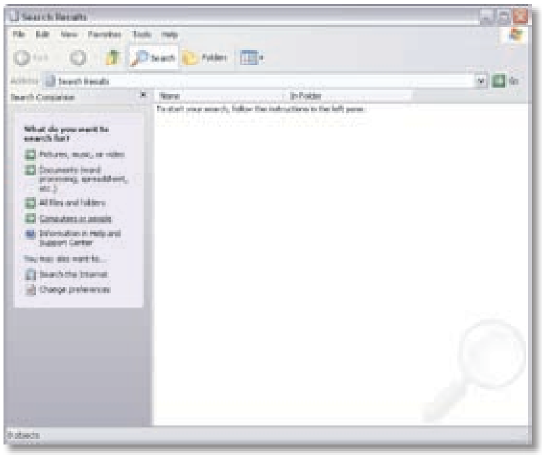
Instructions for Windows XP

1. Click **Start**.
2. Click **Search**.


Internet
Mozilla Firefox
E-mail
Microsoft Office Outlook
Internet Explorer
Microsoft Office Document Imaging
Adobe InDesign CS2 Trial
Command Prompt
SnagIt 8 Editor
Adobe Photoshop CS2
All Programs
My Documents
My Recent Documents
My Computer
Control Panel
Connect To
Printers and Faxes
Help and Support
Search
Run...
Log Off
Shut Down

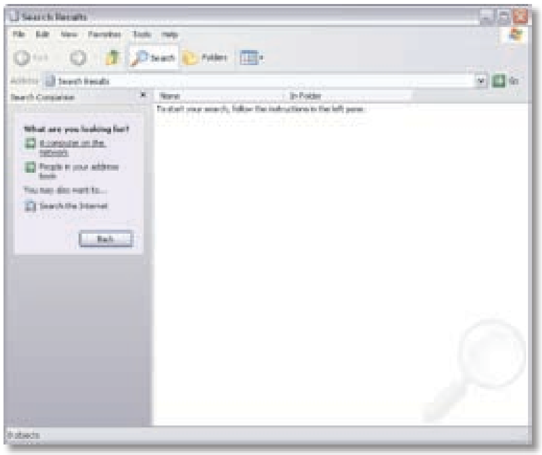
Click Search

3. Click **Computers or people**.


Search Results
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
Address
Search Results
Go
Search Companion
Name
In Folder
To start your search, follow the instructions in the left pane.
What do you want to search for?
Pictures, music, or video
Documents (word processing, spreadsheet, etc.)
All files and folders
Computers or people
Information in Help and Support Center
You may also want to...
Search the Internet
Change preferences

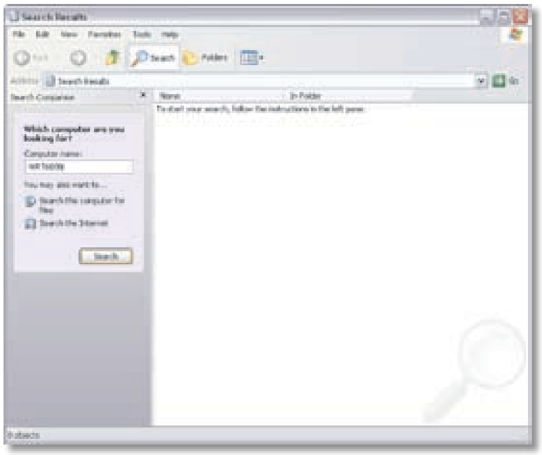
Click Computers or People

4. Click **A computer on the network**.


Search Results
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
Address
Search Results
Go
Search Companion
Name
In Folder
To start your search, follow the instructions in the left pane.
What are you looking for?
A computer on the network
People in your address book
You may also want to...
Search the Internet
Back

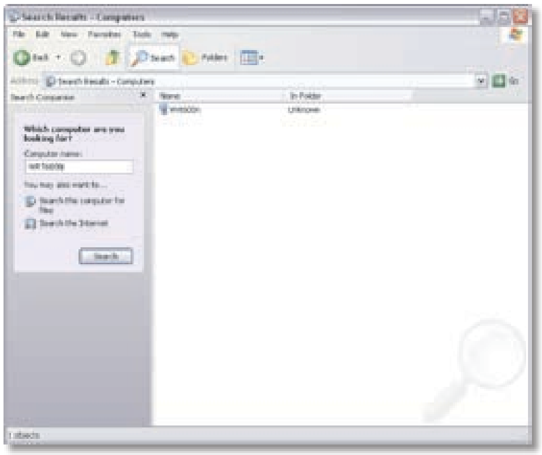
Click A Computer on the Network

5. In the *Computer name* field, enter the server name that you created on the *Storage* > *Administration* screen. The default server name is **WRT610N**. See the *Advanced Configuration* section later in this Appendix for information on how to change the server name. Then click **Search**.


Search Results
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
Address
Search Results
Go
Search Companion
Name
In Folder
To start your search, follow the instructions in the left pane.
Which computer are you looking for?
Computer name:
You may also want to...
Search this computer for files
Search the Internet
Search

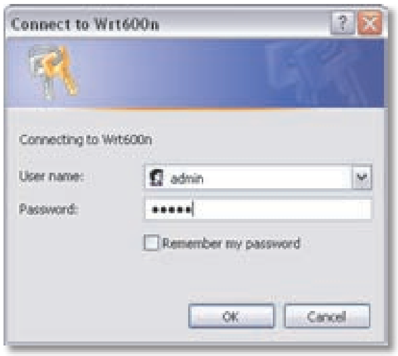
Enter Server Name

6. In the Name column, double-click **Wrt610n**.


Search Results - Computers
File Edit View Favorites Tools Help
Back Search Folders
Search Companion
Name
In Folder
Wrt600n
Unknown
Which computer are you looking for?
Computer name:
WRT600N
You may also want to...
Search this computer for files
Search the Internet
Search
1 objects

Double-Click WRT610N

7. In the *User name* and *Password* fields enter the default User name and password, **admin**. If you want to change the password, see the *Advanced Configuration* section later in this Appendix. Click **OK**.


Connect to Wrt600n

Connecting to Wrt600n

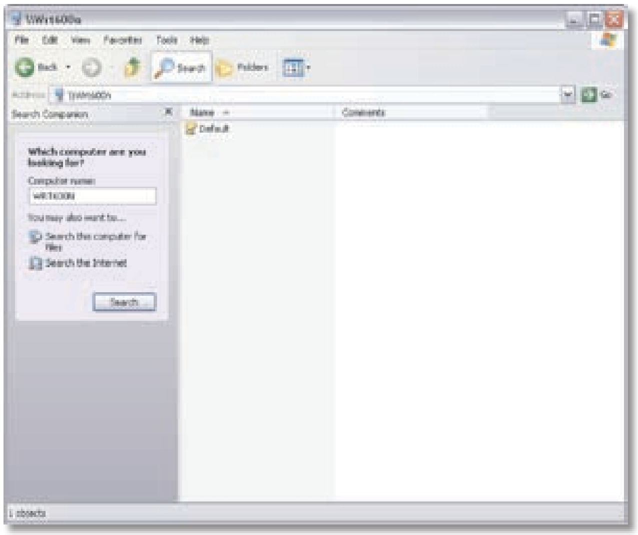
User name: admin

Password: •••••

☐ Remember my password

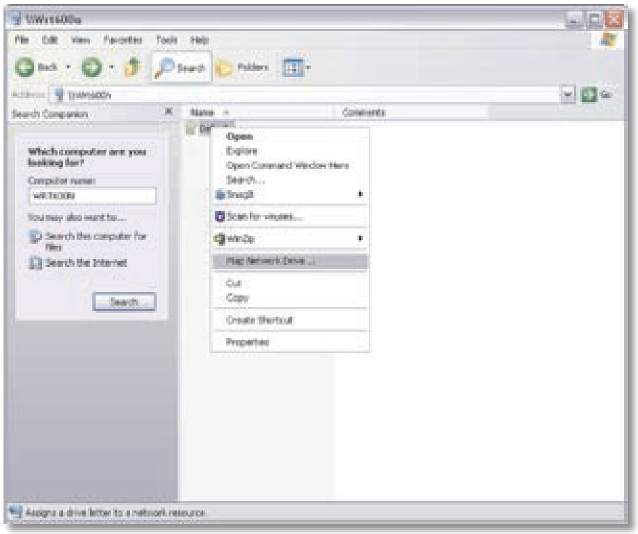
Login Screen

8. The Default shared folder of your USB storage appears. To access your USB storage, double-click **Default**.


\\Wrt600n
File Edit View Favorites Tools Help
Back Search Folders
Address \\Wrt600n
Search Companion
Name
Comments
Default
Which computer are you looking for?
Computer name:
WRT600N
You may also want to...
Search this computer for files
Search the Internet
Search
1 objects

Double-click Default

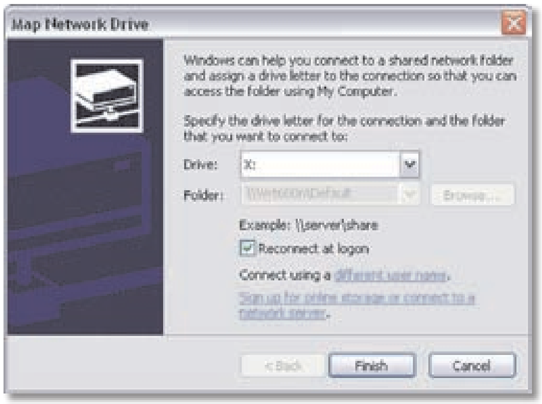
9. To map the Default shared folder to your computer, right-click **Default**. Click **Map Network Drive**.


\\Wrt600n
File Edit View Favorites Tools Help
Back Search Folders
Address \\Wrt600n
Search Companion
Name
Comments
Open
Explore
Open Command Window Here
Search...
SnagIt
Scan for viruses...
WinZip
Map Network Drive...
Cut
Copy
Create Shortcut
Properties
Which computer are you looking for?
Computer name:
WRT600N
You may also want to...
Search this computer for files
Search the Internet
Search
Assigns a drive letter to a network resource

Click Map Network Drive

10. Keep the default Drive letter, or select the letter you want to use from the *Drive* drop-down menu.

    Click **Finish**.


Map Network Drive

Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: X:

Folder: \\Wrt600n\Default

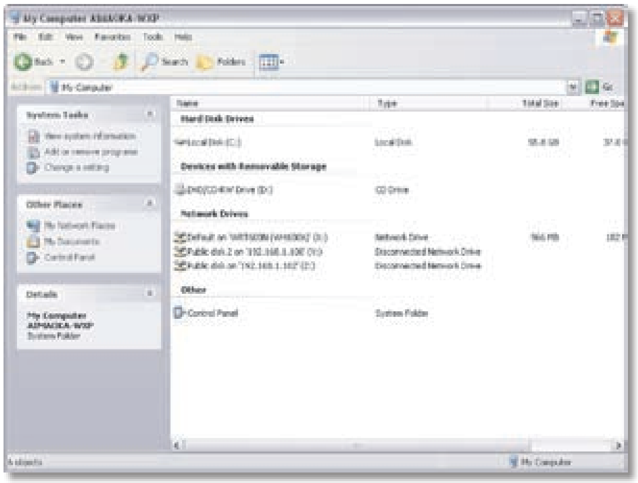
Example: \\server\share

☑ Reconnect at logon

Browse...
Connect using a different user name.
Sign up for online storage or connect to a network server.
< Back
Finish
Cancel

Map Network Drive

11. On your desktop, double-click **My Computer**. The Default shared folder of your USB storage is listed under Network Drives.



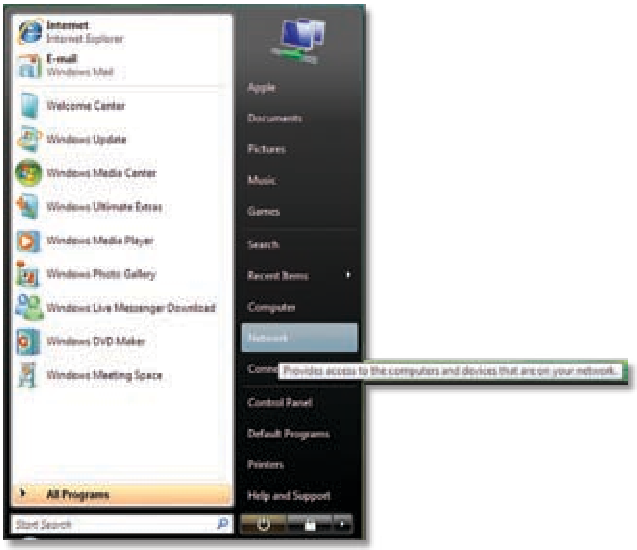
Network Drive

To access your USB storage, double-click the **Default** shared folder. You can use the Default shared folder as another drive on your network.

NOTE: Repeat steps 1-11 to map the USB storage to each XP computer on your network.

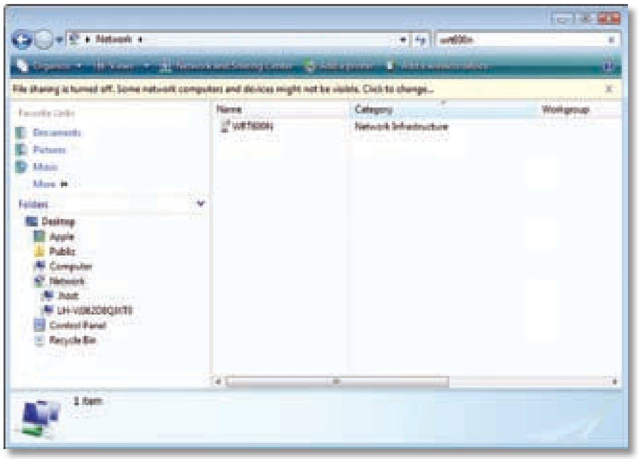
Instructions for Windows Vista

1. Click **Start**.
2. Click **Network**.



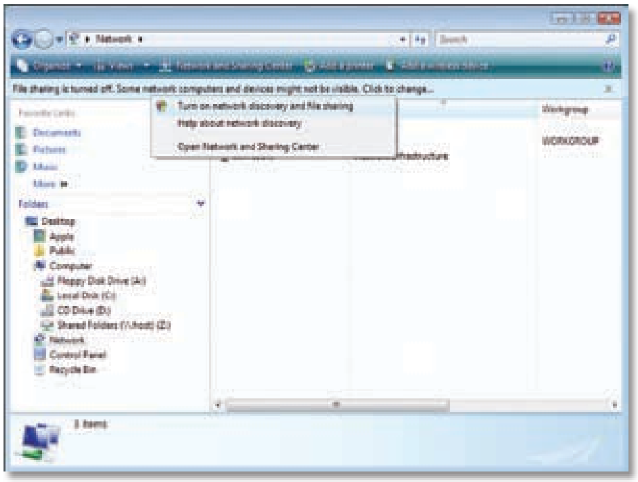
Click Network

3. You will be notified if file sharing is turned off. Click the message.



Click the Message

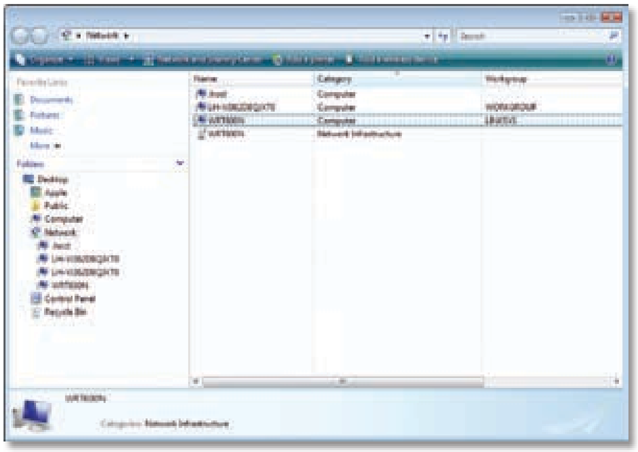
4. Click **Turn on network discovery and file sharing**.



Click Turn on Network Discovery and File Sharing

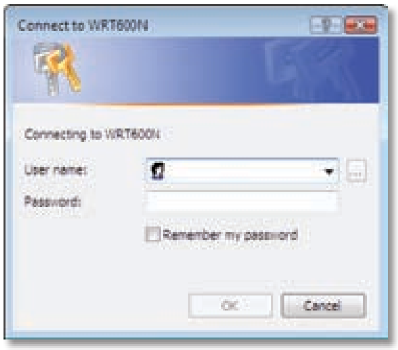
Double-click **WRT610N** listed in the Computer category (do not double-click WRT610N listed in the Network Infrastructure category).

If you do not see the WRT610N listed in the Computer category, then enter the default server name, **WRT610N** in the *Search* field, and press the **Enter** key. See the *Advanced Configuration* section later in this Appendix for information on how to change the server name.


Network
Name
Category
Workgroup
Computer
Network Infrastructure
WORKGROUP
Favorite Links
Documents
Pictures
Music
More
Folders
Desktop
Apple
Public
Computer
Network
Control Panel
Recycle Bin
Category: Network Infrastructure

Double-Click WRT610N (Computer Category)

6. In the *User name* and *Password* fields, enter the default User name and password, **admin**. If you want to change the password, see the *Advanced Configuration* section later in this Appendix. Click **OK**.


Connect to WRT600N
OK
Cancel

Connecting to WRT600N

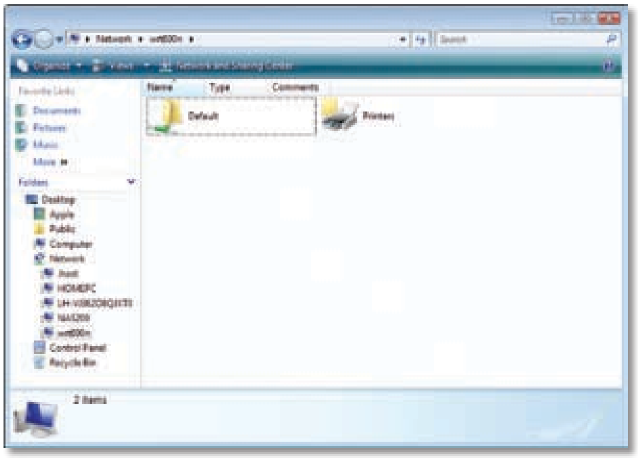
User name:

Password:

☐ Remember my password

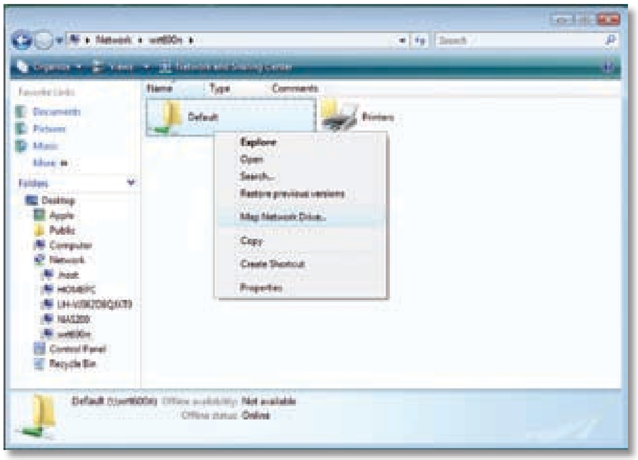
Login Screen

7. The Default shared folder of your USB storage appears. To access your USB storage, double-click **Default**.


Network
wrt600n
Search
Organize
Views
Network and Sharing Center
Name
Type
Comments
Default
Printers
Favorite Links
Documents
Pictures
Music
More
Folders
Desktop
Apple
Public
Computer
Network
HOMEPC
NAS200
wrt600n
Control Panel
Recycle Bin
2 items

Double-Click Default

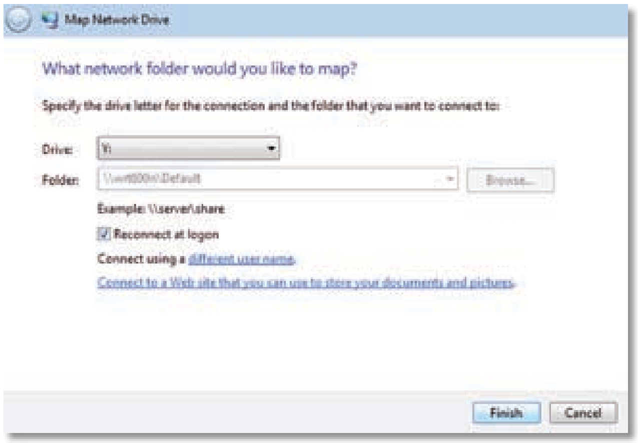
8. To map the Default shared folder to your computer, right-click **Default**. Click **Map Network Drive**.


Network
wrt600n
Default
Printers
Explore
Open
Search...
Restore previous versions
Map Network Drive...
Copy
Create Shortcut
Properties
Default (\\wrt600n) Offline availability: Not available
Offline status: Online

Click Map Network Drive

9. Keep the default Drive letter, or select the letter you want to use from the *Drive* drop-down menu.

   Click **Finish**.


Map Network Drive
Browse...
Finish
Cancel

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Y:

Folder: \\wrt600n\Default

Example: \\server\share

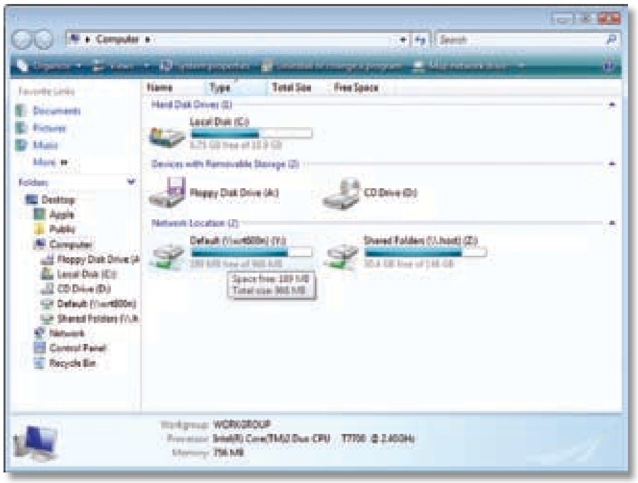
☑ Reconnect at logon

Connect using a different user name.

Connect to a Web site that you can use to store your documents and pictures.

Map Network Drive

10. On your desktop, double-click **My Computer**. The Default shared folder of your USB storage is listed under Network Location.



Network Drive

To access your USB storage, double-click the **Default** shared folder. You can use the Default shared folder as another drive on your network.

NOTE: Repeat steps 1-10 to map the USB storage to each Vista computer on your network,

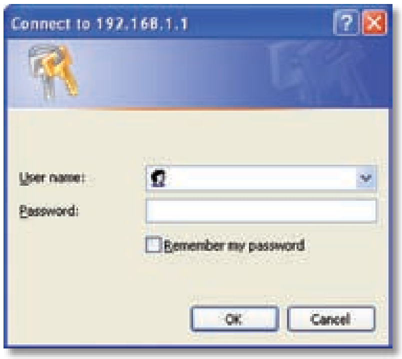
Advanced Configuration (Advanced Users Only)

To manage access to the USB storage device, you can create shared folders, user groups, and user accounts. Follow the instructions in this section.

How to Access the Web-Based Utility

To access the web-based utility, launch the web browser on your computer, and enter the Router's default IP address, **192.168.1.1** or **http://wrt610n.com**, in the *Address* field. Then, press **Enter**.

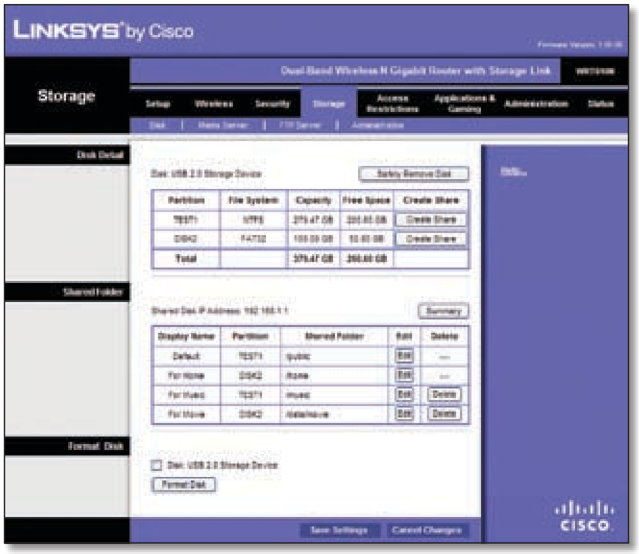
A password request screen will appear. (Non-Windows XP users will see a similar screen.) Leave the *User name* field blank. The first time you open the web-based utility, use the default password **admin**. (You can set a new password from the Administration tab's *Management* screen.) Click **OK** to continue.



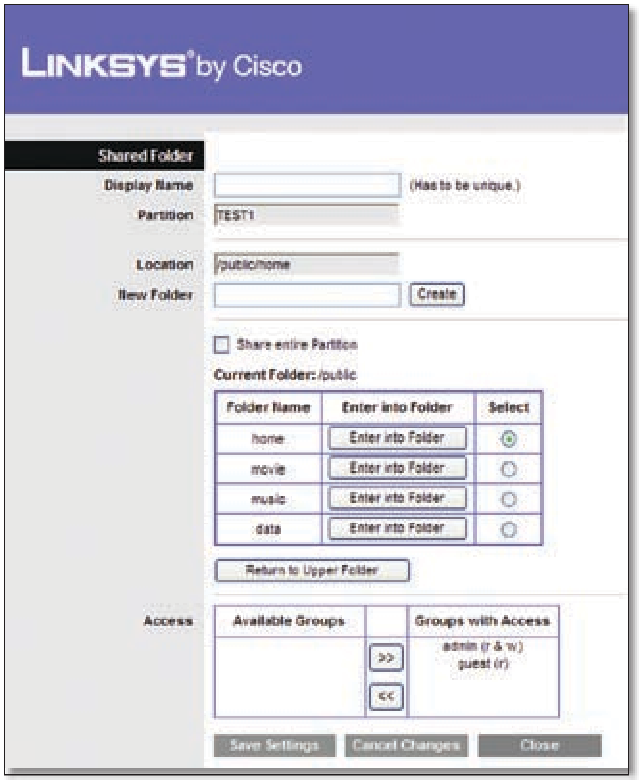
Password Screen

How to Create a Shared Folder

1. Click the **Storage** tab.
2. Click the **Disk** tab.
3. To create a shared folder, click **Create Share**.



Storage > Disk



Display Name (Has to be unique.)

Partition: TEST1

Location: /public/home

New Folder: Create

☐ Share entire Partition

Current Folder: /public

Folder Name	Enter into Folder	Select
home	Enter into Folder	●
movie	Enter into Folder	○
music	Enter into Folder	○
data	Enter into Folder	○

Return to Upper Folder

Access

Available Groups		Groups with Access
		admin (r & w) guest (r)

Shared Folder Screen

Display Name Enter a display name that will appear in the Shared Folder table of the *Disk* screen.

Partion The name of the Partion to share, that you selected in the *Shared Folder* will appear here.

Location The location of the shared folder is displayed.

New Folder To create a new folder, enter a name for the folder and click **Create**.

Share entire Partion To share the entire partition, click the check box for **Share entire Partion**.

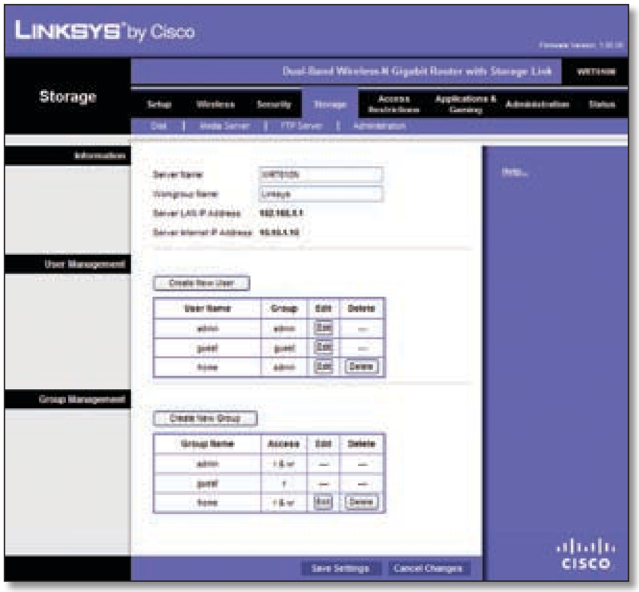
If you don't want to share the entire partition, you can specify the folder you do want to share. Select a folder name to share. To see a sub-folder, click **Enter into Folder**. To return to the previous folder, click **Return to Upper Folder**. To create a new folder, enter a name in the *New Folder* field, then click **Create**.

Access Select the right Access arrows to allow access to a group or the left arrows to remove access to a group. You can allow Read and Write or Read Only access. To add more groups, go to the Storage > Administration s

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Close** to exit the screen.

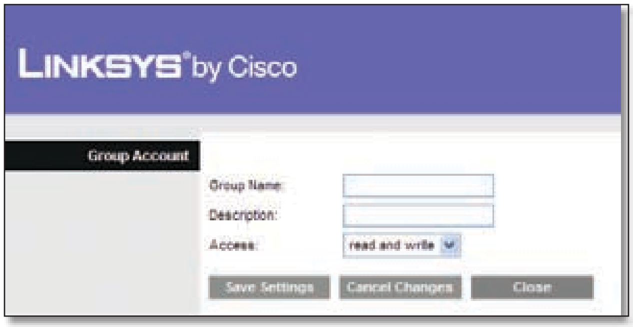
How to Create a User Group

1. Click the **Storage** tab.
2. Click the **Administration** tab.
3. In the Group Management section, click **Create New Group**.



Storage > Administration

4. The *Group Account* screen appears. In the *Group Name* field, enter a name for the new group.



Group Name:

Description:

Access: read and write

Group Account

5. In the *Description* field, enter a description for the new group.
6. From the *Access* drop-down menu, select **read and write** or **read only** access.
7. On the *Group Account* screen, click **Save Settings** to save the new changes, or click **Cancel Changes** to cancel the changes. Click **Close** to close the screen.
8. On the *Administration* screen, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

How to Change the Server Name

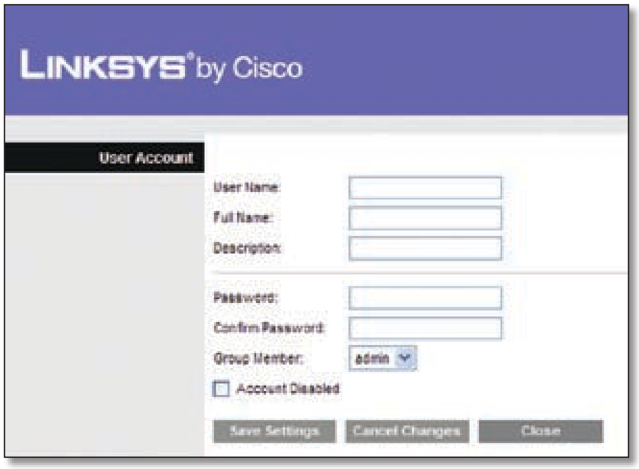
1. Click the **Storage** tab.

2. Click the **Administration** tab.
3. In the *Information, Server Name* field enter a new Server name.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes. Click **Close** to exit the screen.

How to Create a User Account

1. Click the **Storage** tab.
2. Click the **Administration** tab.
3. In the User Management section, click **Create New User**.
4. The *User Account* screen appears. In the *User Name* field, enter a name for the new user.


LINKSYS® by Cisco
User Account
User Name:
Full Name:
Description:
Password:
Confirm Password:
Group Member:
Account Disabled
Save Settings
Cancel Changes
Close

Group Member: admin

☐ Account Disabled

User Account

5. In the *Full Name* field, enter the full name of the new user.
6. In the *Description* field, enter a description for the new user.
7. In the *Password* and *Confirm Password* fields, enter a password.
8. From the *Group Member* drop-down menu, select the appropriate group.
9. If you want to disable the user account, select **Account Disabled**.
10. On the *User Account* screen, click **Save Settings** to save the new changes, or click **Cancel Changes** to cancel the changes. Click **Close** to close the screen.
11. On the *Administration* screen, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Appendix C: Specifications

Model	WRT610N
Standards	Draft 802.11n, 802.11a, 802.11g, 802.11b, 802.3, 802.3u, 802.3ab
Ports	Power, Ethernet, Internet, USB
Button	Reset, Wi-Fi Protected Setup (WPS)
LEDs	Power, USB, Internet, Wireless, Wi-Fi Protected Setup (WPS) Ethernet (1-4)
No. of Antennas	3 Antennas for 2.4 GHz Wireless-N 3 Antennas for 5 GHz Wireless-N
Modulations	802.11b: CCK, QPSK, BPSK 802.11g: OFDM 802.11a: OFDM Wireless-N: BPSK, QPSK, 16-QAM, 64-QAM
RF Pwr (EIRP) in dBm	2.4GHz Wireless-N @ 13.5 ± 1.5dbm (Typical)
	5GHz Wireless-N @ 11 ± 1.5dbm (Typical)
Antenna Gain in dBi	2.4GHz Wireless-N @ 270Mbps @-66 @ 10 PER
	5GHz Wireless-N @ 270Mbps @ -61 @ 10 PER
UPnP	Supported
Security Features	WEP, WPA, WPA2
WEP Key Bits	Up to 128-Bit Encryption

Environmental

Dimensions	8.86" x 1.38" x 7.09" (225 x 35 x 180 mm)
Unit Weight	oz (g)
Power	12V or 1.5A
Certifications	FCC, IC, CE, Wi-Fi a/b/g/draft-n, Vista Premium logo
Operating Temp.	0 to 40°C (32 to 104°F)
Storage Temp.	-20 to 60°C (-4 to 140°F)
Operating Humidity	10 to 80%, Noncondensing
Storage Humidity	5 to 90% Noncondensing

Specifications are subject to change without notice.

Appendix D: Warranty Information

Limited Warranty

Linksys warrants this Linksys hardware product against defects in materials and workmanship under normal use for the Warranty Period, which begins on the date of purchase by the original end-user purchaser and lasts for the period specified below:

- One (1) year for new product
- Ninety (90) days for refurbished product

This limited warranty is non-transferable and extends only to the original end-user purchaser. Your exclusive remedy and Linksys' entire liability under this limited warranty will be for Linksys, at its option, to (a) repair the product with new or refurbished parts, (b) replace the product with a reasonably available equivalent new or refurbished Linksys product, or (c) refund the purchase price of the product less any rebates. Any repaired or replacement products will be warranted for the remainder of the original Warranty Period or thirty (30) days, whichever is longer. All products and parts that are replaced become the property of Linksys.

Exclusions and Limitations

This limited warranty does not apply if: (a) the product assembly seal has been removed or damaged, (b) the product has been altered or modified, except by Linksys, (c) the product damage was caused by use with non-Linksys products, (d) the product has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Linksys, (e) the product has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, (f) the serial number on the Product has been altered, defaced, or removed, or (g) the product is supplied or licensed for beta, evaluation, testing or demonstration purposes for which Linksys does not charge a purchase price or license fee.

ALL SOFTWARE PROVIDED BY LINKSYS WITH THE PRODUCT, WHETHER FACTORY LOADED ON THE PRODUCT OR CONTAINED ON MEDIA ACCOMPANYING THE PRODUCT, IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. Without limiting the foregoing, Linksys does not warrant that the operation of the product or software will be uninterrupted or error free. Also, due to the continual development of new techniques for intruding upon and attacking networks, Linksys does not warrant that the product, software or any equipment, system or network on which the product or software is used will be free of vulnerability to intrusion or attack. The product may include or be bundled with third party software or service offerings. This limited warranty shall not apply to such third party software or service offerings. This limited warranty does not guarantee any continued availability of a third party's service for which this product's use or operation may require.

TO THE EXTENT NOT PROHIBITED BY LAW, ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary by jurisdiction.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF THE THEORY OF LIABILITY (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT (INCLUDING ANY SOFTWARE), EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy provided under this limited warranty fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Obtaining Warranty Service

If you have a question about your product or experience a problem with it, please go to **www.linksys.com/support** where you will find a variety of online support tools and information to assist you with your product. If the product proves defective during the Warranty Period, contact Linksys Technical Support for instructions on how to obtain warranty service. The telephone number for Linksys Technical Support in your area can be found in the product User Guide and at **www.linksys.com**. Have your product serial number and proof of purchase on hand when calling. A DATED PROOF OF ORIGINAL PURCHASE IS REQUIRED TO PROCESS WARRANTY CLAIMS. If you are requested to return your product, you will be given a Return Materials Authorization (RMA) number. You are responsible for properly packaging and shipping your product to Linksys at your cost and risk. You must include the RMA number and a copy of your dated proof of original purchase when returning your product. Products received without a RMA number and dated proof of original purchase will be rejected. Do not include any other items with the product you are returning to Linksys. Defective product covered by this limited warranty will be repaired or replaced and returned to you without charge. Customers outside of the United States of America and Canada are responsible for all shipping and handling charges, custom duties, VAT and other associated taxes and charges. Repairs or replacements not covered under this limited warranty will be subject to charge at Linksys' then-current rates.

Technical Support

This limited warranty is neither a service nor a support contract. Information about Linksys' current technical support offerings and policies (including any fees for support services) can be found at:
www.linksys.com/support.

This limited warranty is governed by the laws of the jurisdiction in which the Product was purchased by you.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623.

Appendix E:
Regulatory Information

FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This product has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. IEEE 802.11b or 802.11g operation of this product in the USA is firmware-limited to channels 1 through 11.

The device for the band 5150-5250 MHz is only for indoor usage to reduce the potential for harmful interference to co-channel mobile satellite systems; the maximum antenna gain of 3.5 dBi permitted (for devices in the band 5725-5825 MHz) to comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate, as stated in section A9.2(3).

Safety Notices

- Caution: To reduce the risk of fire, use only No.26 AWG or larger telecommunication line cord.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

WARNING: This product contains lead, known to the State of California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling.

Wireless Disclaimer

The maximum performance for wireless is derived from IEEE Standard 802.11 specifications. Actual performance can vary, including lower wireless network capacity, data throughput rate, range and coverage. Performance depends on many factors, conditions and variables, including distance from the access point, volume of network traffic, building materials and construction, operating system used, mix of wireless products used, interference and other adverse conditions.

Industry Canada Statement

This Class B digital apparatus complies with Canadian ICES-003 and RSS210.

Operation is subject to the following two conditions:

1. This device may not cause interference and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

Industry Canada Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Restrictions in the 5 GHz Band

The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.

No.	Antenna Type	For 2.4 GHz Gain (dBi)	For 5 GHz Gain (dBi)	Antenna Connector
1	PIFA	< = 4	< = 3.5	NA
2	PIFA	< = 4	< = 3.5	NA
3	PIFA	< = 4	< = 3.5	NA

Avis d'Industrie Canada

Cet appareil numérique de la classe B est conforme aux normes NMB-003 et RSS210 du Canada.

L'utilisation de ce dispositif est autorisée seulement aux conditions suivantes :

1. il ne doit pas produire de brouillage et
2. il doit accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif. Le dispositif a été conçu pour fonctionner avec une antenne ayant un gain maximum de 2 dBi. Les règlements d'Industrie Canada interdisent strictement l'utilisation d'antennes dont le gain est supérieur à cette limite. L'impédance requise de l'antenne est de 50 ohms.
   Afin de réduire le risque d'interférence aux autres utilisateurs, le type d'antenne et son gain doivent être choisis de façon à ce que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne soit pas supérieure au niveau requis pour obtenir une communication satisfaisante.

Avis d'Industrie Canada concernant l'exposition aux radiofréquences

Ce matériel est conforme aux limites établies par IC en matière d'exposition aux radiofréquences dans un environnement non contrôlé. Ce matériel doit être installé et utilisé à une distance d'au moins 20 cm entre l'antenne et le corps de l'utilisateur.

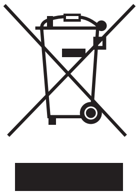
L'émetteur ne doit pas être placé près d'une autre antenne ou d'un autre émetteur, ou fonctionner avec une autre antenne ou un autre émetteur.

Avis de non-responsabilité concernant les appareils sans fil

Les performances maximales pour les réseaux sans fil sont tirées des spécifications de la norme IEEE 802.11. Les performances réelles peuvent varier, notamment en fonction de la capacité du réseau sans fil, du débit de la transmission de données, de la portée et de la couverture. Les performances dépendent de facteurs, conditions et variables multiples, en particulier de la distance par rapport au point d'accès, du volume du trafic réseau, des matériaux utilisés dans le bâtiment et du type de construction, du système d'exploitation et de la combinaison de produits sans fil utilisés, des interférences et de toute autre condition défavorable.

User Information for Consumer Products Covered by EU Directive 2002/96/EC on Waste Electric and Electronic Equipment (WEEE)

This document contains important information for users with regards to the proper disposal and recycling of Linksys products. Consumers are required to comply with this notice for all electronic products bearing the following symbol:



English - Environmental Information for Customers in the European Union

European Directive 2002/96/EC requires that the equipment bearing this symbol ⊠ on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

Български (Bulgarian) - Информация относно опазването на околната среда за потребители в Европейския съюз

Европейска директива 2002/96/EC изисква уредите, носещи този символ ⊠ върху изделието и/или опаковката му, да не се изхвърля т с несортирани битови отпадъци. Символът обозначава, че изделието трябва да се изхвърля отделно от сметосъбирането на обикновените битови отпадъци. Ваша е отговорността този и другите електрически и електронни уреди да се изхвърлят в предварително определени от държавните или общински органи специализирани пунктове за събиране. Правилното изхвърляне и рециклиране ще спомогнат да се предотвратят евентуални вредни за околната среда и здравето на населението последствия. За по-подробна информация относно изхвърлянето на вашите стари уреди се обърнете към местните власти, службите за сметосъбиране или магазина, от който сте закупили уреда.

Ceština (Czech) - Informace o ochraně životního prostředí pro zákazníky v zemích Evropské unie

Evropská směrnice 2002/96/ES zakazuje, aby zařízení označené tímto symbolem ⊠ na produktu anebo na obalu bylo likvidováno s netříděným komunálním odpadem. Tento symbol udává, že daný produkt musí být likvidován odděleně od běžného komunálního odpadu. Odpovídáte za likvidaci tohoto produktu a dalších elektrických a elektronických zařízení prostřednictvím určených sběrných míst stanovených vládou nebo místními úřady. Správná likvidace a recyklace pomáhá předcházet potenciálním negativním dopadům na životní prostředí a lidské zdraví. Podrobnější informace o likvidaci starého vybavení si laskavě vyžádejte od místních úřadů, podniku zabývajícího se likvidací komunálních odpadů nebo obchodu, kde jste produkt zakoupili.

Dansk (Danish) - Miljøinformation for kunder i EU

EU-direktiv 2002/96/EF kræver, at udstyr der bærer dette symbol ⊠ på produktet og/eller emballagen ikke må bortskaffes som usorteret kommunalt affald. Symbolet betyder, at dette produkt skal bortskaffes adskilt fra det almindelige husholdningsaffald. Det er dit ansvar at bortskaffe dette og andet elektrisk og elektronisk udstyr via bestemte indsamlingssteder udpeget af staten eller de lokale myndigheder. Korrekt bortskaffelse og genvinding vil hjælpe med til at undgå mulige skader for miljøet og menneskers sundhed. Kontakt venligst de lokale myndigheder, renovationstjenesten eller den butik, hvor du har købt produktet, angående mere detaljeret information om bortskaffelse af dit gamle udstyr.

Deutsch (German) - Umweltinformation für Kunden innerhalb der Europäischen Union

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist ⊠, nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

Eesti (Estonian) - Keskkonnaalane informatsioon Euroopa Liidus asuvatele klientidele

Euroopa Liidu direktiivi 2002/96/EÜ nõuete kohaselt on seadmeid, millel on tootel või pakendil käesolev sümbol 🗑, keelatud kõrvaldada koos sorteerimata olmejäätmetega. See sümbol näitab, et toode tuleks kõrvaldada eraldi tavalistest olmejäätmevoogudest. Olete kohustatud kõrvaldama käesoleva ja ka muud elektri- ja elektroonikaseadmed riigi või kohalike ametiasutuste poolt ette nähtud kogumispunktide kaudu. Seadmete korrektne kõrvaldamine ja ringlussevõtt aitab vältida võimalikke negatiivseid tagajärgi keskkonnale ning inimeste tervisele. Vanade seadmete kõrvaldamise kohta täpsema informatsiooni saamiseks võtke palun ühendust kohalike ametiasutustega, jäätmekäitlusfirmaga või kauplusega, kust te toote ostsite.

Español (Spanish) - Información medioambiental para clientes de la Unión Europea

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo 🗑 en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.

ξλληνικά (Greek) - Στοιχεία περιβαλλοντικής προστασίας για πελάτες εντός της Ευρωπαϊκής Ένωσης

Η Κοινοτική Οδηγία 2002/96/EC απαιτεί ότι ο εξοπλισμός ο οποίος φέρει αυτό το σύμβολο 🗑 στο προϊόν και/ή στη συσκευασία του δεν πρέπει να απορρίπτεται μαζί με τα μικτά κοινοτικά απορρίμματα. Το σύμβολο υποδεικνύει ότι αυτό το προϊόν θα πρέπει να απορρίπτεται ξεχωριστά από τα συνήθη οικιακά απορρίμματα. Είστε υπεύθυνος για την απόρριψη του παρόντος και άλλου ηλεκτρικού και ηλεκτρονικού εξοπλισμού μέσω των καθορισμένων εγκαταστάσεων συγκέντρωσης απορριμμάτων οι οποίες παρέχονται από το κράτος ή τις αρμόδιες τοπικές αρχές. Η σωστή απόρριψη και ανακύκλωση συμβάλλει στην πρόληψη πιθανών αρνητικών συνεπειών για το περιβάλλον και την υγεία. Για περισσότερες πληροφορίες σχετικά με την απόρριψη του παλιού σας εξοπλισμού, παρακαλώ επικοινωνήστε με τις τοπικές αρχές, τις υπηρεσίες απόρριψης ή το κατάστημα από το οποίο αγοράσατε το προϊόν.

Français (French) - Informations environnementales pour les clients de l'Union européenne

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole 🗑 sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L'élimination et le recyclage en bonne et due forme ont pour but de lutter contre l'impact néfaste potentiel de ce type de produits sur l'environnement et la santé publique. Pour plus d'informations sur le mode d'élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l'endroit où vous avez acheté le produit.

Italiano (Italian) - Informazioni relative all'ambiente per i clienti residenti nell'Unione Europea

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo 🗑 sul prodotto e/o sull'imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l'ambiente e per la salute dell'essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

Latviešu valoda (Latvian) - Ekoloģiska informācija klientiem Eiropas Savienības jurisdikcijā

Direktīvā 2002/96/EK ir prasība, ka aprīkojumu, kam pievienota zīme 🗑 uz paša izstrādājuma vai uz tā iesaiņojuma, nedrīkst izmest nešķirotā veidā kopā ar komunālajiem atkritumiem (tiem, ko rada vietēji iedzīvotāji un uzņēmumi). Šī zīme nozīmē to, ka šī ierīce ir jāizmet atkritumos tā, lai tā nenonāktu kopā ar parastiem mājsaimniecības atkritumiem. Jūsu pienākums ir šo un citas elektriskas un elektroniskas ierīces izmest atkritumos, izmantojot īpašus atkritumu savākšanas veidus un līdzekļus, ko nodrošina valsts un pašvaldību iestādes. Ja izmešana atkritumos un pārstrāde tiek veikta pareizi, tad mazinās iespējamais kaitējums dabai un cilvēku veselībai. Sīkākas ziņas par novecojuša aprīkojuma izmešanu atkritumos jūs varat saņemt vietējā pašvaldībā, atkritumu savākšanas dienestā, kā arī veikalā, kur iegādājāties šo izstrādājumu.

Lietuvškai (Lithuanian) - Aplinkosaugos informacija, skirta Europos Sąjungos vartotojams

Europos direktyva 2002/96/EC numato, kad įrangos, kuri ir 🗑 kurios pakuotė yra pažymėta šiuo simboliu (įveskite simbolį), negalima šalinti kartu su nerūšiuotomis komunalinėmis atliekomis. Šis simbolis rodo, kad gaminį reikia šalinti atskirai nuo bendro buitinių atliekų srauto. Jūs privalote užtikrinti, kad ši ir kita elektros ar elektroninė įranga būtų šalinama per tam tikras nacionalinės ar vietinės valdžios nustatytas atliekų rinkimo sistemas. Tinkamai šalinant ir perdirbant atliekas, bus išvengta galimos žalos aplinkai ir žmonių sveikatai. Daugiau informacijos apie jūsų senos įrangos šalinimą gali pateikti vietinės valdžios institucijos, atliekų šalinimo tarnybos arba parduotuvės, kuriose įsigijote tą gaminį.

Malti (Maltese) - Informazzjoni Ambjentali għal Klijenti fl-Unjoni Ewropea

Id-Direttiva Ewropea 2002/96/KE titlob li t-tagħmir li jkun fih is-simbolu 🗑 fuq il-prodott u/jew fuq l-ippakkjar ma jistax jintrema ma' skart muniċipali li ma ġiex isseparat. Is-simbolu jindika li dan il-prodott għandu jintrema separatament minn ma' l-iskart domestiku regolari. Hija responsabbiltà tiegħek li tarmi dan it-tagħmir u kull tagħmir ieħor ta' l-elettriku u elettroniku permezz ta' faċilitajiet ta' ġbir appuntati apposta mill-gvern jew mill-awtoritajiet lokali. Ir-rimi b'mod korrett u r-riċiklaġġ jgħin jipprevjeni konsegwenzi negattivi potenzjali għall-ambjent u għas-saħħa tal-bniedem. Għal aktar informazzjoni dettaljata dwar ir-rimi tat-tagħmir antik tiegħek, jekk jogħġbok ikkuntattja lill-awtoritajiet lokali tiegħek, is-servizzi għar-rimi ta' l-iskart, jew il-ħanut minn fejn xtrajt il-prodott.

Magyar (Hungarian) - Környezetvédelmi információ az európai uniós vásárlók számára

A 2002/96/EC számú európai uniós irányelv megkívánja, hogy azokat a termékeket, amelyeken, és/vagy amelyek csomagolásán az alábbi címke 🗑 megjelenik, tilos a többi szelektálatlan lakossági hulladékkal együtt kidobni. A címke azt jelöli, hogy az adott termék kidobásakor a szokványos háztartási hulladékelszállítási rendszerektõl elkülönített eljárást kell alkalmazni. Az Ön felelõssége, hogy ezt, és más elektromos és elektronikus berendezéseit a kormányzati vagy a helyi hatóságok által kijelölt gyűjtõredszereken keresztül számolja fel. A megfelelõ hulladékfeldolgozás segít a környezetre és az emberi egészségre potenciálisan ártalmas negatív hatások megelõzésében. Ha elavult berendezéseinek felszámolásához további részletes információra van szüksége, kérjük, lépjen kapcsolatba a helyi hatóságokkal, a hulladékfeldolgozási szolgálattal, vagy azzal üzlettel, ahol a terméket vásárolta.

Nederlands (Dutch) - Milieu-informatie voor klanten in de Europese Unie

De Europese Richtlijn 2002/96/EC schrijft voor dat apparatuur die is voorzien van dit symbool 🗑 op het product of de verpakking, niet mag worden ingezameld met niet-gescheiden huishoudelijk afval. Dit symbool geeft aan dat het product apart moet worden ingezameld. U bent zelf verantwoordelijk voor de vernietiging van deze en andere elektrische en elektronische apparatuur via de daarvoor door de landelijke of plaatselijke overheid aangewezen inzamelingskanalen. De juiste vernietiging en recycling van deze apparatuur voorkomt mogelijke negatieve gevolgen voor het milieu en de gezondheid. Voor meer informatie over het vernietigen van uw oude apparatuur neemt u contact op met de plaatselijke autoriteiten of afvalverwerkingsdienst, of met de winkel waar u het product hebt aangeschaft.

Norsk (Norwegian) - Miljøinformasjon for kunder i EU

EU-direktiv 2002/96/EF krever at utstyr med følgende symbol 🗑 avbildet på produktet og/eller pakningen, ikke må kastes sammen med usortert avfall. Symbolet indikerer at dette produktet skal håndteres atskilt fra ordinær avfallsinnsamling for husholdningsavfall. Det er ditt ansvar å kvitte deg med dette produktet og annet elektrisk og elektronisk avfall via egne innsamlingsordninger slik myndighetene eller kommunene bestemmer. Korrekt avfallshåndtering og gjenvinning vil være med på å forhindre mulige negative konsekvenser for miljø og helse. For nærmere informasjon om håndtering av det kasserte utstyret ditt, kan du ta kontakt med kommunen, en innsamlingsstasjon for avfall eller butikken der du kjøpte produktet.

Polski (Polish) - Informacja dla klientów w Unii Europejskiej o przepisach dotyczących ochrony środowiska

Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem 🗑 znajdującym się na produkcie i/lub jego opakowaniu nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w punktach odbioru wyznaczonych przez władze krajowe lub lokalne. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu, prosimy zwrócić się do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

Português (Portuguese) - Informação ambiental para clientes da União Europeia

A Directiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É da sua responsabilidade eliminar este e qualquer outro equipamento eléctrico e electrónico através das instalações de recolha designadas pelas autoridades governamentais ou locais. A eliminação e reciclagem correctas ajudarão a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, contacte as autoridades locais, os serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Română (Romanian) - Informaţii de mediu pentru clienţii din Uniunea Europeană

Directiva europeană 2002/96/CE impune ca echipamentele care prezintă acest simbol pe produs şi/sau pe ambalajul acestuia să nu fie casate împreună cu gunoiul menajer municipal. Simbolul indică faptul că acest produs trebuie să fie casat separat de gunoiul menajer obişnuit. Este responsabilitatea dvs. să casaţi acest produs şi alte echipamente electrice şi electronice prin intermediul unităţilor de colectare special desemnate de guvern sau de autorităţile locale. Casarea şi reciclarea corecte vor ajuta la prevenirea potenţialelor consecinţe negative asupra sănătăţii mediului şi a oamenilor. Pentru mai multe informaţii detaliate cu privire la casarea acestui echipament vechi, contactaţi autorităţile locale, serviciul de salubrizare sau magazinul de la care aţi achiziţionat produsul.

Slovenčina (Slovak) - Informácie o ochrane životného prostredia pre zákazníkov v Európskej únii

Podľa európskej smernice 2002/96/ES zariadenie s týmto symbolom na produkte a/alebo jeho balení nesmie byť likvidované spolu s netriedeným komunálnym odpadom. Symbol znamená, že produkt by sa mal likvidovať oddelene od bežného odpadu z domácností. Je vašou povinnosťou likvidovať toto i ostatné elektrické a elektronické zariadenia prostredníctvom špecializovaných zberných zariadení určených vládou alebo miestnymi orgánmi. Správna likvidácia a recyklácia pomôže zabrániť prípadným negatívnym dopadom na životné prostredie a zdravie ľudí. Ak máte záujem o podrobnejšie informácie o likvidácii starého zariadenia, obráťte sa, prosím, na miestne orgány, organizácie zaoberajúce sa likvidáciou odpadov alebo obchod, v ktorom ste si produkt zakúpili.

Slovenčina (Slovene) - Okoljske informacije za stranke v Evropski uniji

Evropska direktiva 2002/96/EC prepoveduje odlaganje opreme, označene s tem simbolom – na izdelku in/ali na embalaži – med običajne, nerazvrščene odpadke. Ta simbol opozarja, da je treba izdelek odvreči ločeno od preostalih gospodinjskih odpadkov. Vaša odgovornost je, da to in preostalo električno in elektronsko opremo odnesete na posebna zbirališča, ki jih določijo državne ustanove ali lokalna uprava. S pravilnim odlaganjem in recikliranjem boste preprečili morebitne škodljive vplive na okolje in zdravje ljudi. Če želite izvedeti več o odlaganju stare opreme, se obrnite na lokalno upravo, odpad ali trgovino, kjer ste izdelek kupili.

Suomi (Finnish) - Ympäristöä koskevia tietoja EU-alueen asiakkaille

EU-direktiivi 2002/96/EY edellyttää, että jos laitteistossa on tämä symboli itse tuotteessa ja/tai sen pakkauksessa, laitteistoa ei saa hävittää lajittelemattoman yhdyskuntajätteen mukana. Symboli merkitsee sitä, että tämä tuote on hävitettävä erillään tavallisesta kotitalousjätteestä. Sinun vastuullasi on hävittää tämä elektroniikkatuote ja muut vastaavat elektroniikkatuotteet viemällä tuote tai tuotteet viranomaisten määräämään keräyspisteeseen. Laitteiston oikea hävittäminen estää mahdolliset kielteiset vaikutukset ympäristöön ja ihmisten terveyteen. Lisätietoja vanhan laitteiston oikeasta hävitystavasta saa paikallisilta viranomaisilta, jätteenhävityspalvelusta tai siitä myymälästä, josta ostit tuotteen.

Svenska (Swedish) - Miljöinformation för kunder i Europeiska unionen

Det europeiska direktivet 2002/96/EC kräver att utrustning med denna symbol på produkten och/eller förpackningen inte får kastas med osorterat kommunalt avfall. Symbolen visar att denna produkt bör kastas efter att den avskiljts från vanligt hushållsavfall. Det faller på ditt ansvar att kasta denna och annan elektrisk och elektronisk utrustning på fastställda insamlingsplatser utsedda av regeringen eller lokala myndigheter. Korrekt kassering och återvinning skyddar mot eventuella negativa konsekvenser för miljön och personhälsa. För mer detaljerad information om kassering av din gamla utrustning kontaktar du dina lokala myndigheter, avfallshanteringen eller butiken där du köpte produkten.

WEB: For additional information, please visit **www.linksys.com**

Appendix F: Software License Agreement

Software in Linksys Products

This product from Cisco-Linksys LLC or from one of its affiliates Cisco Systems-Linksys (Asia) Pte Ltd. or Cisco-Linksys K.K. ("Linksys") contains software (including firmware) originating from Linksys and its suppliers and may also contain software from the open source community. Any software originating from Linksys and its suppliers is licensed under the Linksys Software License Agreement contained at Schedule 1 below. You may also be prompted to review and accept that Linksys Software License Agreement upon installation of the software.

Any software from the open source community is licensed under the specific license terms applicable to that software made available by Linksys at **www.linksys.com/gpl** or as provided for in Schedules 2 and 3 below.

Where such specific license terms entitle you to the source code of such software, that source code is upon request available at cost from Linksys for at least three years from the purchase date of this product and may also be available for download from **www.linksys.com/gpl**. For detailed license terms and additional information on open source software in Linksys products please look at the Linksys public web site at: **www.linksys.com/gpl/** or Schedule 2 below as applicable.

BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THE SOFTWARE LICENSE AGREEMENTS BELOW. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

Software Licenses

The software Licenses applicable to software from Linksys are made available at the Linksys public web site at: **www.linksys.com** and **www.linksys.com/gpl/** respectively. For your convenience of reference, a copy of the Linksys Software License Agreement and the main open source code licenses used by Linksys in its products are contained in the Schedules below.

Schedule 1 - Linksys Software License Agreement

THIS LICENSE AGREEMENT IS BETWEEN YOU AND CISCO-LINKSYS LLC OR ONE OF ITS AFFILIATES CISCO SYSTEMS-LINKSYS (ASIA) PTE LTD. OR CISCO-LINKSYS K.K. ("LINKSYS") LICENSING THE SOFTWARE INSTEAD OF CISCO-LINKSYS LLC. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

License. Subject to the terms and conditions of this Agreement, Linksys grants the original end user purchaser of the Linksys product containing the Software ("You") a nonexclusive license to use the Software solely as embedded in or (where authorized in the applicable documentation) for communication with such product. This license may not be sublicensed, and is not transferable except to a person or entity to which you transfer ownership of the complete Linksys product containing the Software, provided you permanently transfer all rights under this Agreement and do not retain any full or partial copies of the Software, and the recipient agrees to the terms of this Agreement.

"Software" includes, and this Agreement will apply to (a) the software of Linksys or its suppliers provided in or with the applicable Linksys product, and (b) any upgrades, updates, bug fixes or modified versions ("Upgrades") or backup copies of the Software supplied to You by Linksys or an authorized reseller, provided you already hold a valid license to the original software and have paid any applicable fee for the Upgrade.

Protection of Information. The Software and documentation contain trade secrets and/or copyrighted materials of Linksys or its suppliers. You will not copy or modify the Software or decompile, decrypt, reverse engineer or disassemble the Software (except to the extent expressly permitted by law notwithstanding this provision), and You will not disclose or make available such trade secrets or copyrighted material in any form to any third party. Title to and ownership of the Software and documentation and any portion thereof, will remain solely with Linksys or its suppliers.

Collection and Processing of Information. You agree that Linksys and/or its affiliates may, from time to time, collect and process information about your Linksys product and/or the Software and/or your use of either in order (i) to enable Linksys to offer you Upgrades; (ii) to ensure that your Linksys product and/or the Software is being used in accordance with the terms of this Agreement; (iii) to provide improvements to the way Linksys delivers technology to you and to other Linksys customers; (iv) to enable Linksys to comply with the terms of any agreements it has with any third parties regarding your Linksys product and/or Software and/or (v) to enable Linksys to comply with all applicable laws and/or regulations, or the requirements of any regulatory authority or government agency. Linksys and/ or its affiliates may collect and process this information provided that it does not identify you personally. Your use of your Linksys product and/or the Software constitutes this consent by you to Linksys and/or its affiliates' collection and use of such information and, for EEA customers, to the transfer of such information to a location outside the EEA.

Software Upgrades etc. If the Software enables you to receive Upgrades, you may elect at any time to receive these Upgrades either automatically or manually. If you elect to receive Upgrades manually or you otherwise elect not to receive or be notified of any Upgrades, you may expose your Linksys product and/or the Software to serious security threats and/or some features within your Linksys product and/or Software may become inaccessible. There may be circumstances where we apply an Upgrade automatically in order to comply with changes in legislation, legal or regulatory requirements or as a result of requirements to comply with the terms of any agreements Linksys has with any third parties regarding your Linksys product and/or the Software. You will always be notified of any Upgrades being delivered to you. The terms of this license will apply to any such Upgrade unless the Upgrade in question is accompanied by a separate license, in which event the terms of that license will apply.

Open Source Software. The GPL or other open source code incorporated into the Software and the open source license for such source code are available for free download at **http://www.linksys.com/gpl**. If You would like a copy of the GPL or other open source code in this Software on a CD, Linksys will mail to You a CD with such code for $9.99 plus the cost of shipping, upon request.

Term and Termination. You may terminate this License at any time by destroying all copies of the Software and documentation. Your rights under this License will terminate immediately without notice from Linksys if You fail to comply with any provision of this Agreement.

Limited Warranty. The warranty terms and period specified in the applicable Linksys Product User Guide shall also apply to the Software.

Disclaimer of Liabilities. IN NO EVENT WILL LINKSYS OR ITS SUPPLIERS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF CAUSE (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

Export. Software, including technical data, may be subject to U.S. export control laws and regulations and/or export or import regulations in other countries. You agree to comply strictly with all such laws and regulations.

U.S. Government Users. The Software and documentation qualify as "commercial items" as defined at 48 C.F.R. 2.101 and 48 C.F.R. 12.212. All Government users acquire the Software and documentation with only those rights herein that apply to non-governmental customers.

General Terms. This Agreement will be governed by and construed in accordance with the laws of the State of California, without reference to conflict of laws principles. The United Nations Convention on Contracts for the International Sale of Goods will not apply. If any portion of this Agreement is found to be void or unenforceable, the remaining provisions will remain in full force and effect. This Agreement constitutes the entire agreement between the parties with respect to the Software and supersedes any conflicting or additional terms contained in any purchase order or elsewhere.

END OF SCHEDULE 1

Schedule 2

If this Linksys product contains open source software licensed under Version 2 of the "GNU General Public License" then the license terms below in this Schedule 2 will apply to that open source software. The license terms below in this Schedule 2 are from the public web site at **http://www.gnu.org/copyleft/gpl.html**

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright © 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software–to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

   If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

END OF SCHEDULE 2

Schedule 3

If this Linksys product contains open source software licensed under the OpenSSL license:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (**http://www.openssl.org/**).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

In addition, if this Linksys product contains open source software licensed under the OpenSSL license then the license terms below in this Schedule 3 will apply to that open source software. The license terms below in this Schedule 3 are from the public web site at **http://www.openssl.org/source/license.html**.

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (**http://www.openssl.org/**)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (**http://www.openssl.org/**)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com)All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

END OF SCHEDULE 3